Proof of Concept Technical Solution

for the *Marconi Law Firm, LLC*.

(WordPress Website)

Project Background: Assume that you are an entrepreneur and that you own your own Information Technology (IT) consulting firm. You have recently acquired a new client called "**Marconi Law Firm**".

As part of your client's contract & paid agreement, you are to deliver full documentation for their upcoming WordPress Website Hosting project implementation. This documentation includes a Proof-of-Concept Technical Solution which documents all software, hardware, and network configuration details. Assume that the finished document will be used in-house by the Marconi Law Firm and will be referenced by their in-house IT department---after the project has been successfully completed.

Jalif E Vazquez Melendez

Cyber-Ware Solutions LLC.

Preface

This document will serve as proof of concept to Mr. Marconi for creating his WordPress website for his law firm and as audit documentation.

The purpose of audit documentation is to provide a comprehensive record of the organization's information technology infrastructure and security controls and processes. It plays a crucial role in providing transparency, accountability, and QA/QC regarding an organization's cybersecurity controls and practices. It enables organizations to demonstrate compliance, identify areas for improvement, and make informed decisions to strengthen their overall organizational cybersecurity.

Audit documentation serves several important purposes:

- **Compliance**: Evidence that an organization has undergone a thorough examination of its systems. It helps validate that the organization has implemented appropriate controls to protect its information systems and sensitive data.

- **Validation**: Verification of the effectiveness and adequacy of cybersecurity controls. It provides detailed information about the design, implementation, and operation of these controls, enabling reviewers to assess their reliability and identify any gaps or weaknesses.

- **Records Maintenance**: Historical record of cybersecurity audits conducted over time. It enables organizations to track their progress, identify trends, and evaluate the effectiveness actions taken. It also serves as reference for future audits and allows auditors to understand the current cybersecurity implemented and facilitates a more targeted approach to future cybersecurity updates and audits.

- **Decision-making Support**: Valuable insights and information that can support decision-making processes. It allows management to make informed decisions about allocating resources, prioritizing cybersecurity investments, and addressing identified risks and vulnerabilities.

Table of Contents

Inventory

EQUIPMENT	OPERATIING SYSTEM	ADDITIONAL INFO	IP ADDRESS
Router/Custom Network	-	-	10.10.229.1
Docker	CentOS 7	Ghost Container	10.10.229.11
NginX Reverse Proxy	Rocky 8	Reverse Proxy	10.10.229.10
WordPress	Ubuntu	LAMP Stack running WordPress	10.10.229.12

Custom Network

NETWORK NAME	SUBNET IP	SUBNET MASK	DNS	GATEWAY
ITE229	10.10.229.0	255.255.255.0	10.10.229.1	10.10.229.1

IDs and Passwords

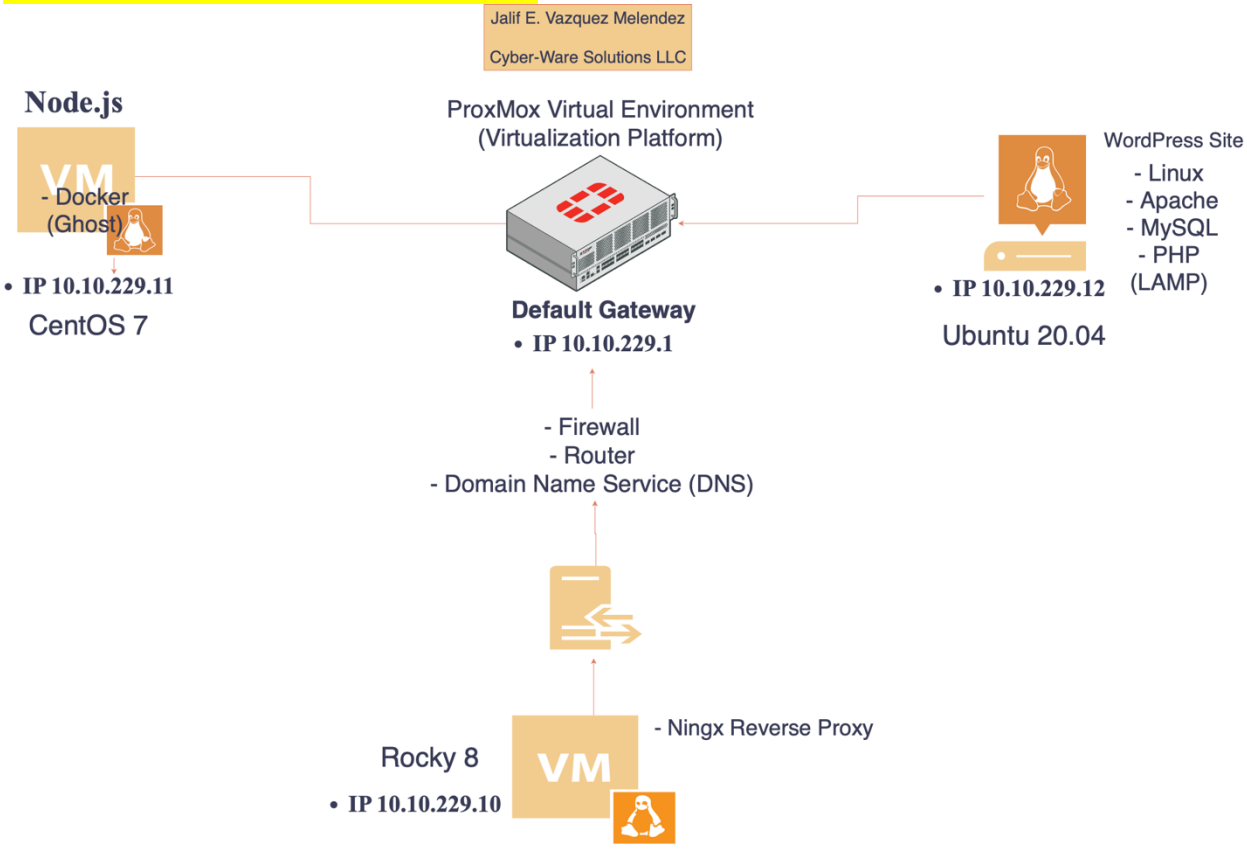
ACCOUNT	USER ID	PASSWORD
CentOS 7 Root User	root	Fullsail1!
Rocky 8 Root User	root	Fullsail1!
MySQL Root User	root@localhost	[randompassword]
MySQL WordPress User	WordPressUser	[randompassword]
WordPress Admin	admin	[randompassword]

IMPORTANT: To earn full credit, original formatting of this document must remain in place. In addition, ALL screenshots must include a "full view", including your ProxMox title bar with your username showing.

Network Topology Diagram

IMPORTANT: Be sure your name is at the TOP of your diagram. Diagrams without your name will result in an automatic zero (0) grade for *each weekly milestone* (Weeks 1-4).

1. CREATE & INSERT YOUR OWN IMAGE OF A "**STAR**" TOPOLOGY HERE – USE DRAW.IO, VISIO, WHATEVER DIAGRAMING TOOL YOU PREFER.



2. Based on what you've learned and the research you've conducted during Week #1, write at least a **75-word summary** (or more words) explaining the purpose of each Virtual Machine (VM) to Mr. Marconi: 1) how the network traffic works, 2) software is installed on each machine, and 3) how the firewall works. Remember, that Mr. Marconi is a Lawyer and not necessarily technical. This means that your summary should be easy to understand for a non-technical Client.

Our team has the idea of bringing your desired deliverables for this project to fruition in a robust yet understandable and manageable. The ProxMox Virtual Environment is a software solution that allows you to create and manage virtual machines (VMs) and containers. It provides a platform for running multiple operating systems that is the same as computers and applications in a single physical place. Simply put, it is a virtualization platform that helps you optimize your computer hardware resources by consolidating various of them on a single place we call a server. We are using that environment to install the necessary systems to provide the project expectations while ensuring we provide performance, security, and scalability.

I emphasize the importance of what we are installing over the next four weeks and installing Node.js. Let's begin by explaining what Node.js is and the scalable network infrastructure we will use to run our applications. The second application would be Docker, and among other applications, we are installing Ghost and Nginx. Still, we are installing Nginx as a reverse proxy in our upcoming project, as it can be used in many ways. Nginx as a reverse proxy is essential because it helps to improve performance, scalability, and security. By handling incoming requests and directing them to the appropriate backend server, Nginx ensures that our application is secure and optimized for maximum performance. By installing Node.js, we can ensure that our project runs smoothly and efficiently. By doing so, we can benefit from several advantages that will help us build a high-performance and secure application. In summary, by installing Docker as a Node.js to use it with Ghost and Nginx as a reverse proxy, we can build a high-performance, secure, and scalable application that meets the law firm's needs. Ghost is a modern publishing platform that allows us to create and manage content.

Your diagram & summary should include the following details:

- Include all VMs, IP Addresses, Software installation on each machine, Firewall, and arrows/lines to show the network traffic flow & other connections based on FSO requirements;

- Once you have created your own Network Topology Diagram and Summary, DELETE the notes above and replace it with your own quick “network traffic summary” for the Marconi Law Firm.

- Plan to update Topology Summary and Diagram during each weekly milestone---as we ADD software installations & server configurations to this project.

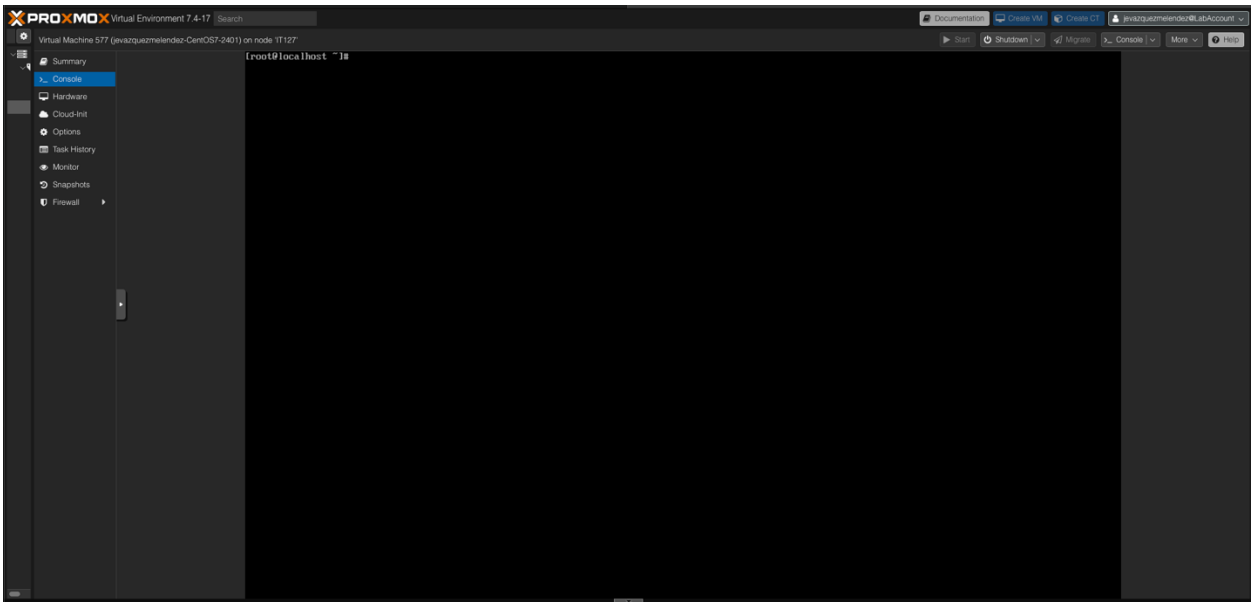
- **NOTE**: If you need additional info “**STAR**” Network Topology Diagrams, please do some research online---starting with links below:
  https://www.linkedin.com/learning/cisco-networking-foundations-fundamentals-of-cisco-networking/examples-of-network-topologies?autoplay=true&resume=false&u=50813145

  https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/

IMPORTANT: To earn full credit, original formatting of this document must remain in place. In addition, ALL screenshots must include a “full view”, including your ProxMox title bar with your username showing.

Milestone #1: Node.js App (Ghost) on Docker

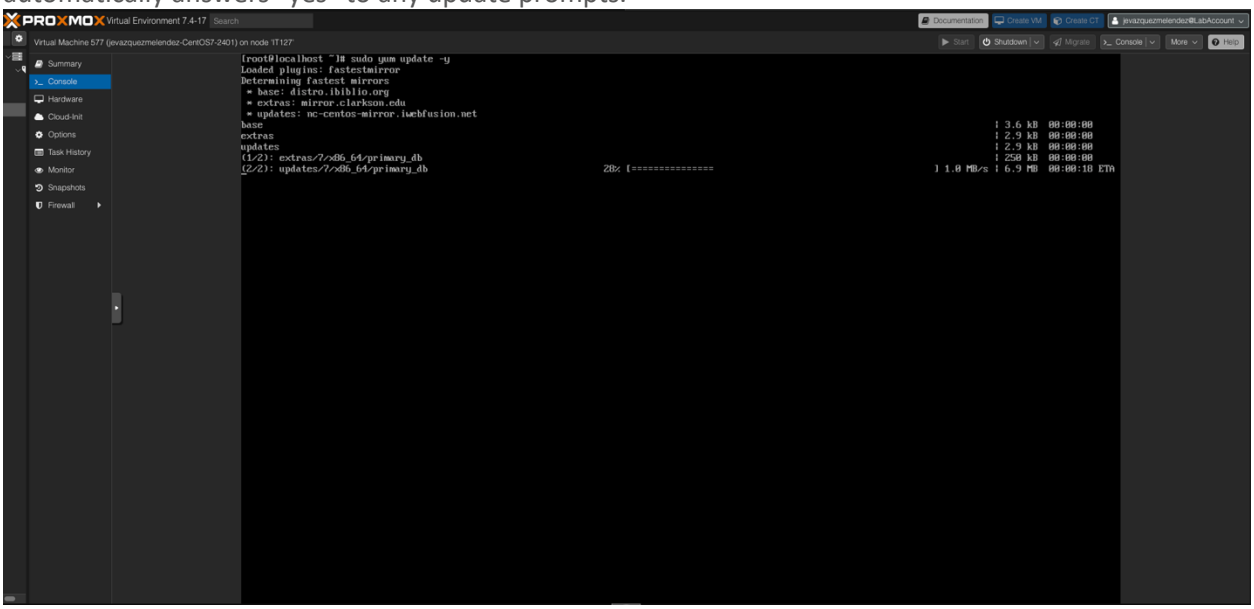
Show screenshot of your CentOS 7 Console in VE



Update CentOS

sudo yum update -y

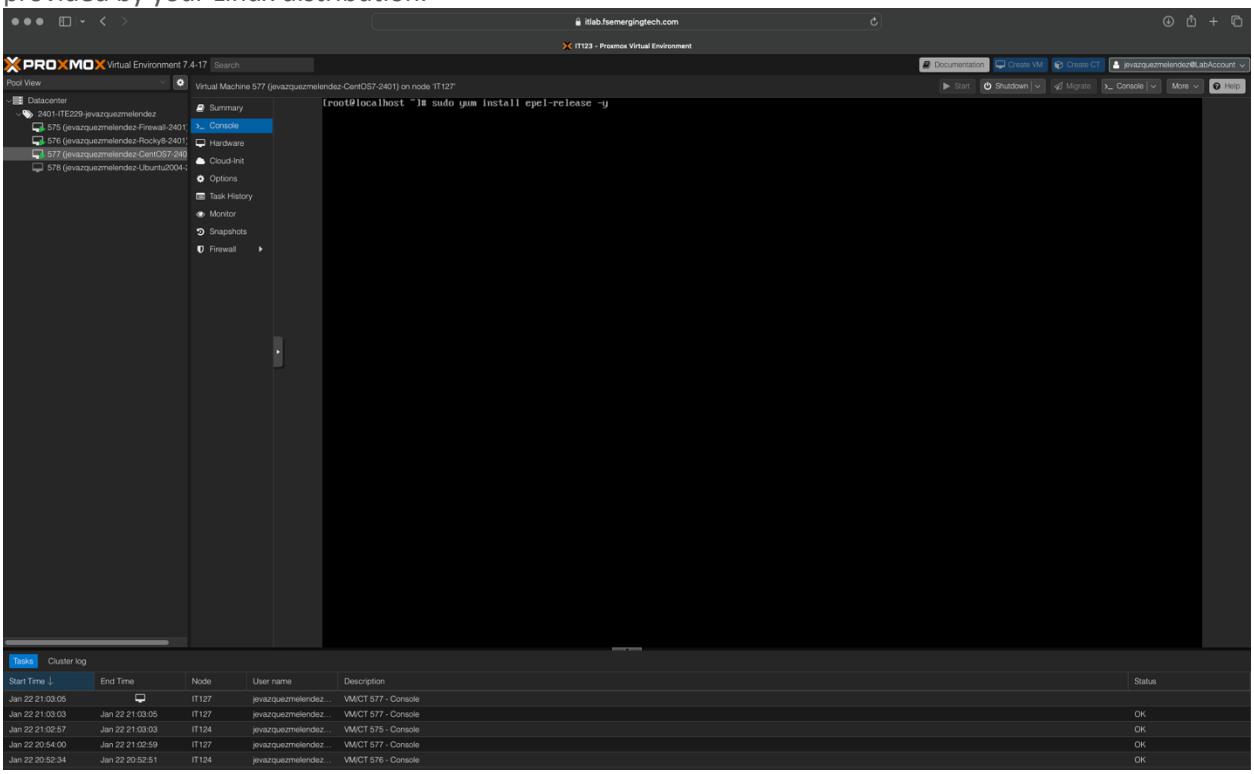
The command sudo yum update -y is used to update the installed packages on your system. The -y flag automatically answers "yes" to any update prompts.



Install EPEL Packages

sudo yum install epel-release -y

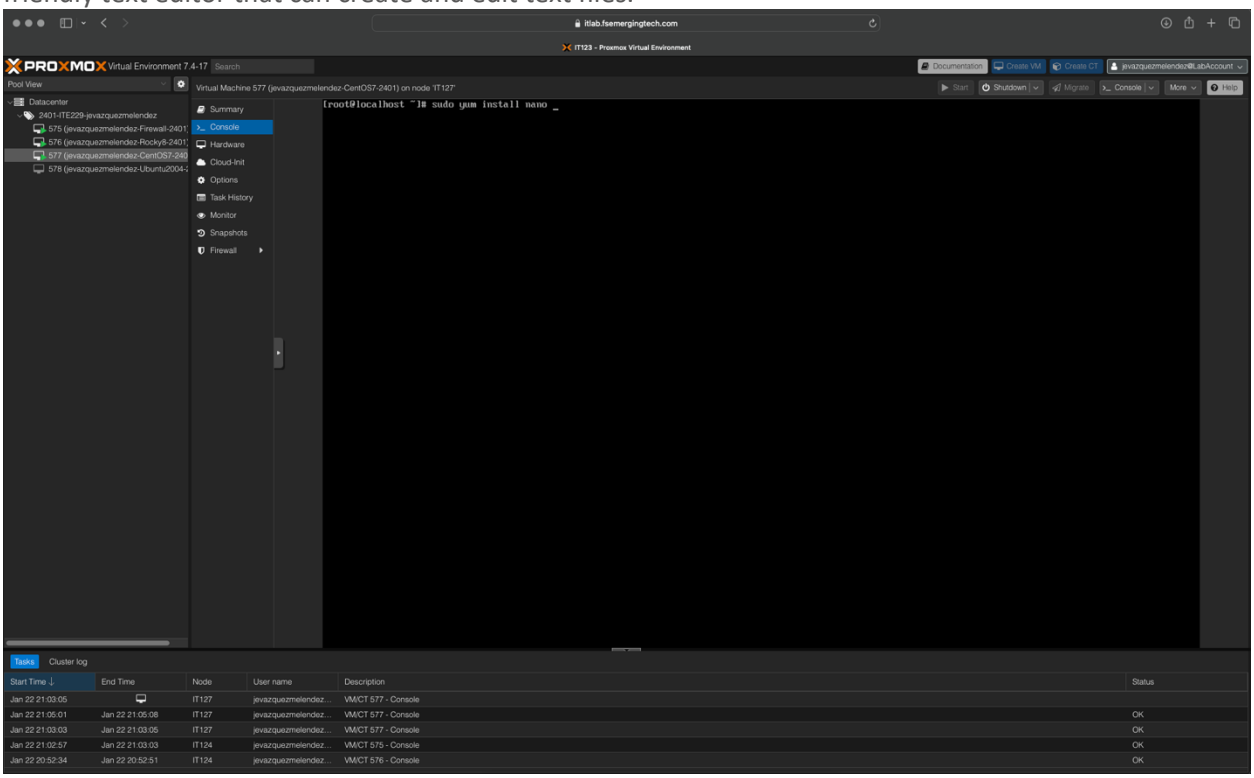
The command sudo yum install epel-release installs your system's Extra Packages for Enterprise Linux (EPEL) repository. This repository contains additional software packages not included in the default repositories provided by your Linux distribution.



Install Nano Editor

$ sudo yum install nano -y

The command sudo yum install nano installs the Nano text editor on your system. Nano is a simple, user-friendly text editor that can create and edit text files.



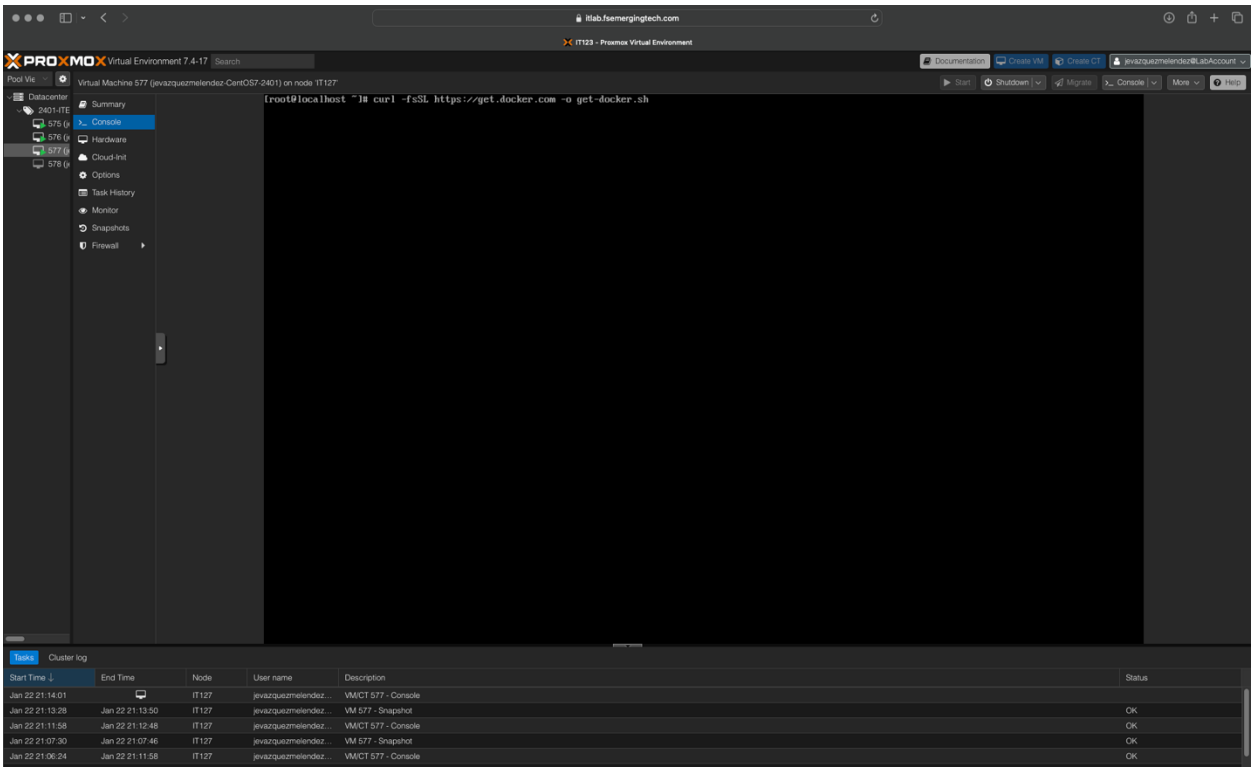
Docker CE

Install required packages

Type the following commands to download docker ce.

sudo -fsSL https://get.docker.com -o get-docker.sh

These commands, typed as follows, allow us to install all the necessary packages to use the docker This command container on our CentOS VM.

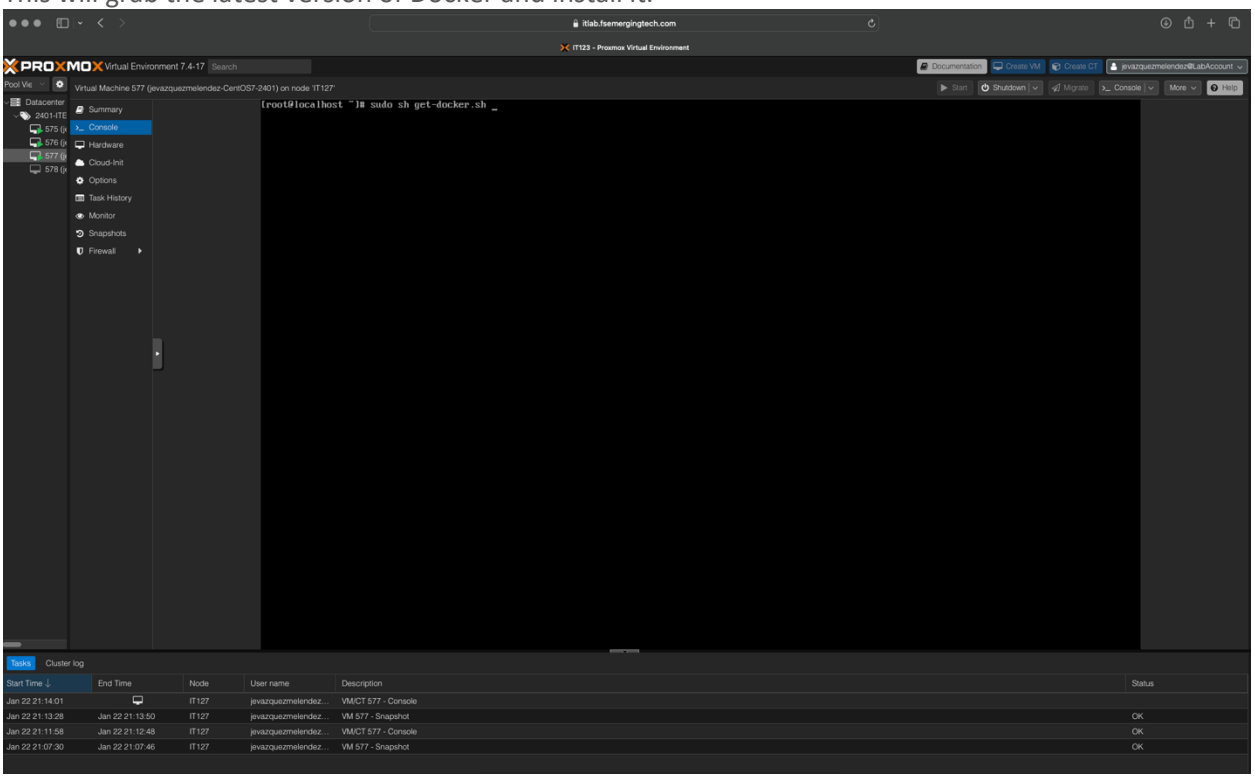


Install Docker CE

To install the latest version, run the following:

sudo sh get-docker.sh

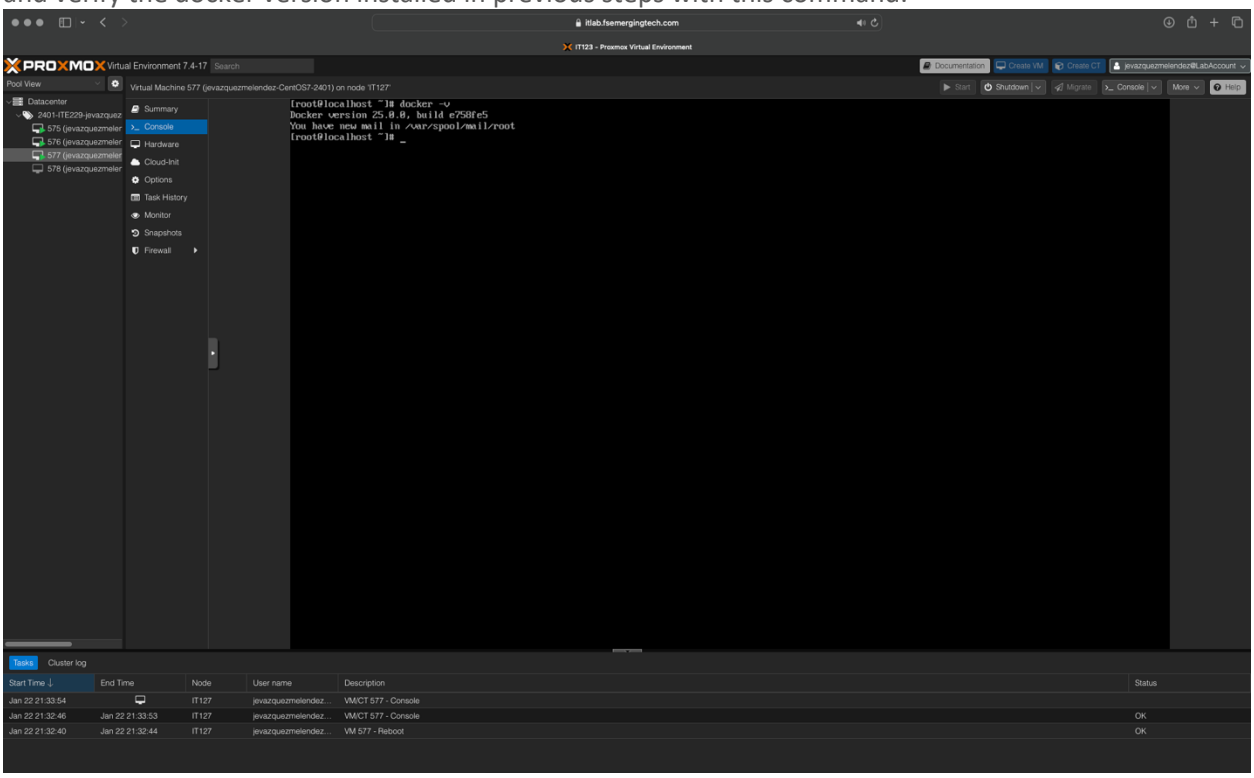
This will grab the latest version of Docker and install it.



Verify docker version

docker -v

This command is used to verify the version of the current docker program installed. We can stay up to date and verify the docker version installed in previous steps with this command.

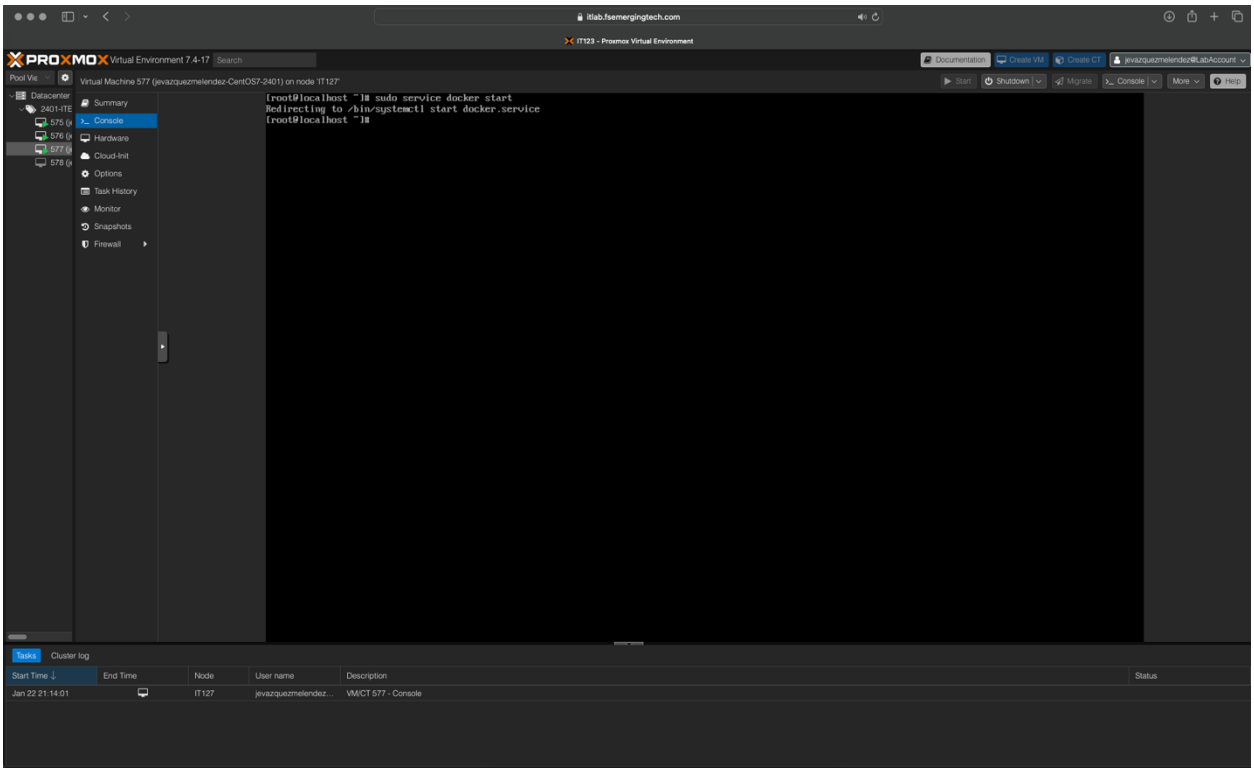


Initialize Docker

Start Docker

sudo systemctl start docker

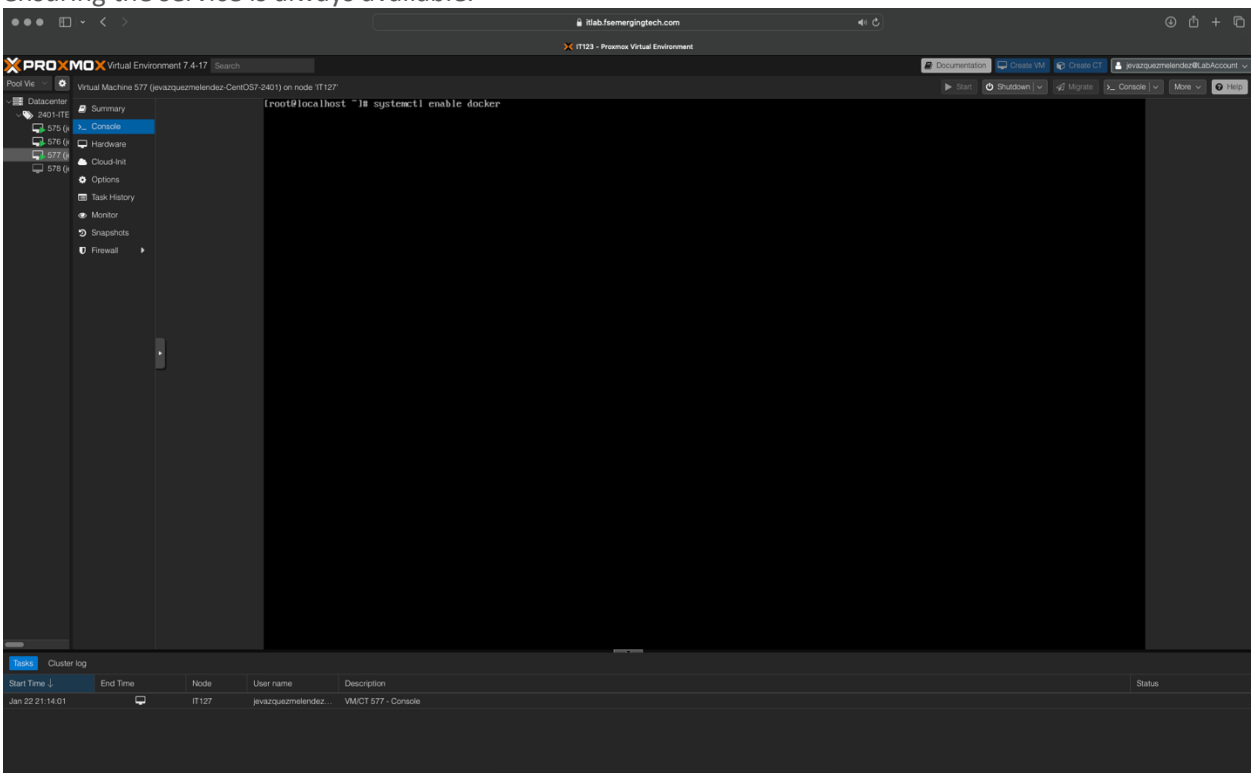
The command sudo systemctl starts docker. Starts the Docker service on a Linux system, allowing you to run Docker containers.



Enable Docker

sudo systemctl enable docker

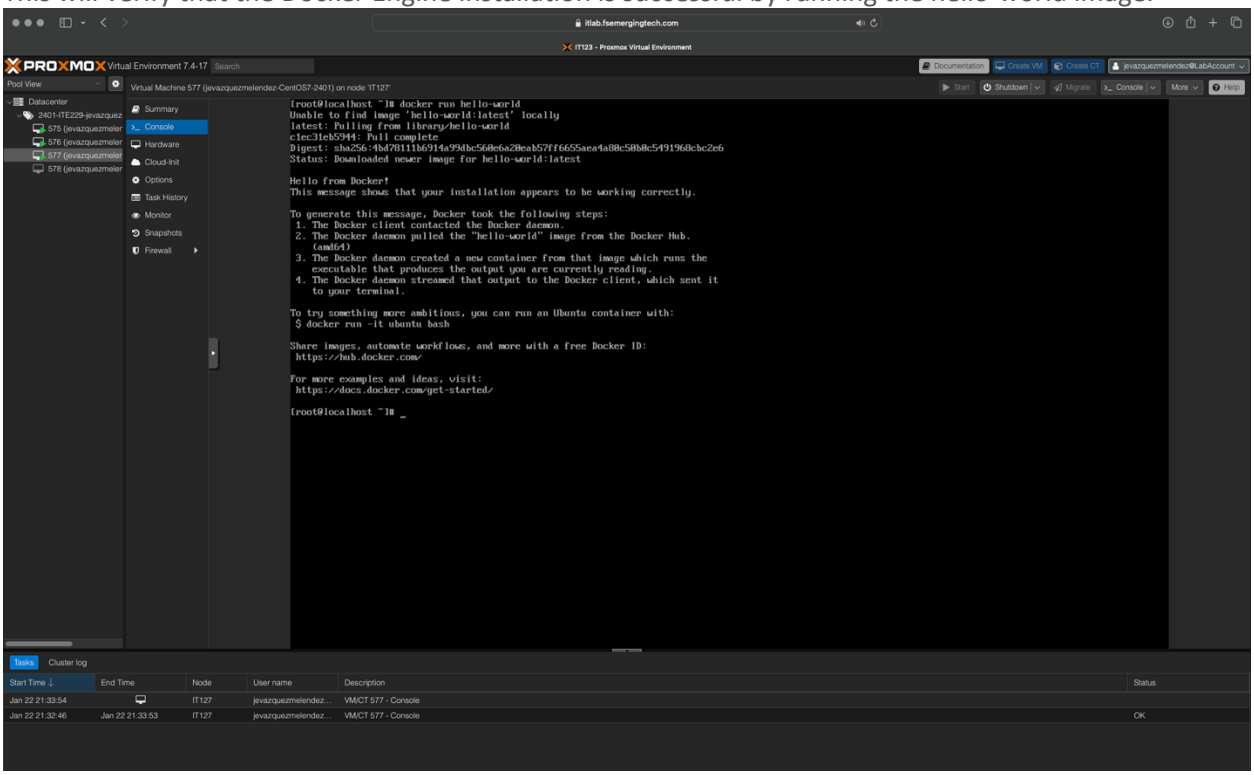
The command sudo systemctl enables us to set docker to start automatically when the system boots up, ensuring the service is always available.



Test Docker (hello-world)

sudo docker run hello-world

This will verify that the Docker Engine installation is successful by running the hello-world image.



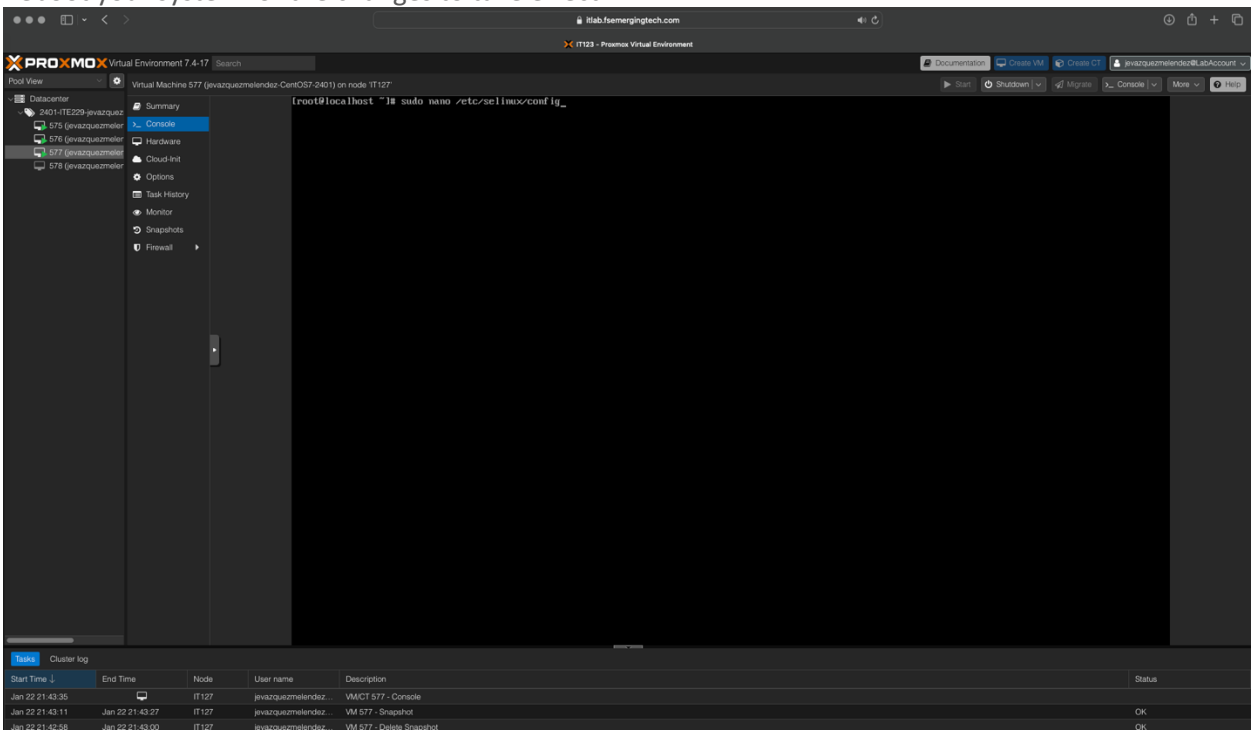
Disable SELinux

sudo nano /etc/selinux/config

To disable SELinux by editing its configuration file, you can follow these steps:
Run the following command to open the SELinux configuration file in the Nano text editor with root privileges:

sudo nano /etc/selinux/config

Locate the line that starts with SELINUX= and change its value to disabled.
Save the changes by pressing Ctrl + X and pressing enter.
Reboot your system for the changes to take effect.

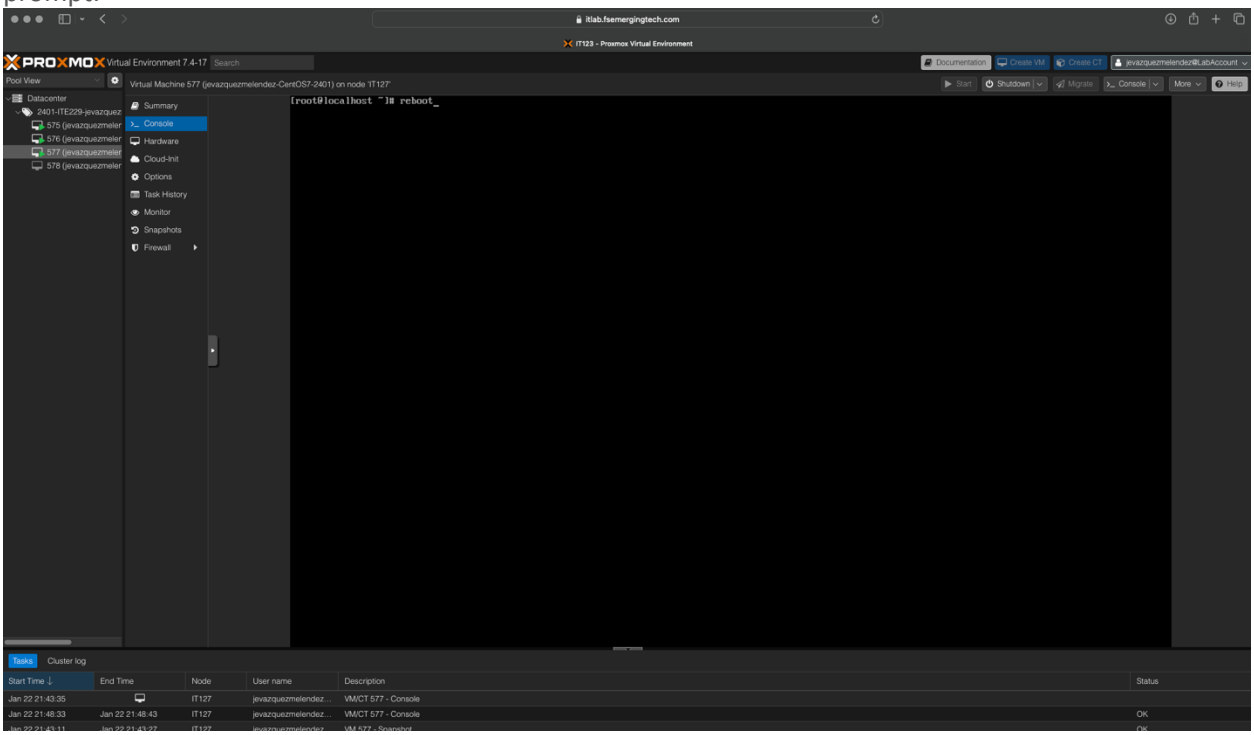


Reboot VM

Reboot VM

reboot

This command is used to reboot or reset a Virtual Machine from the terminal shell using a command prompt.

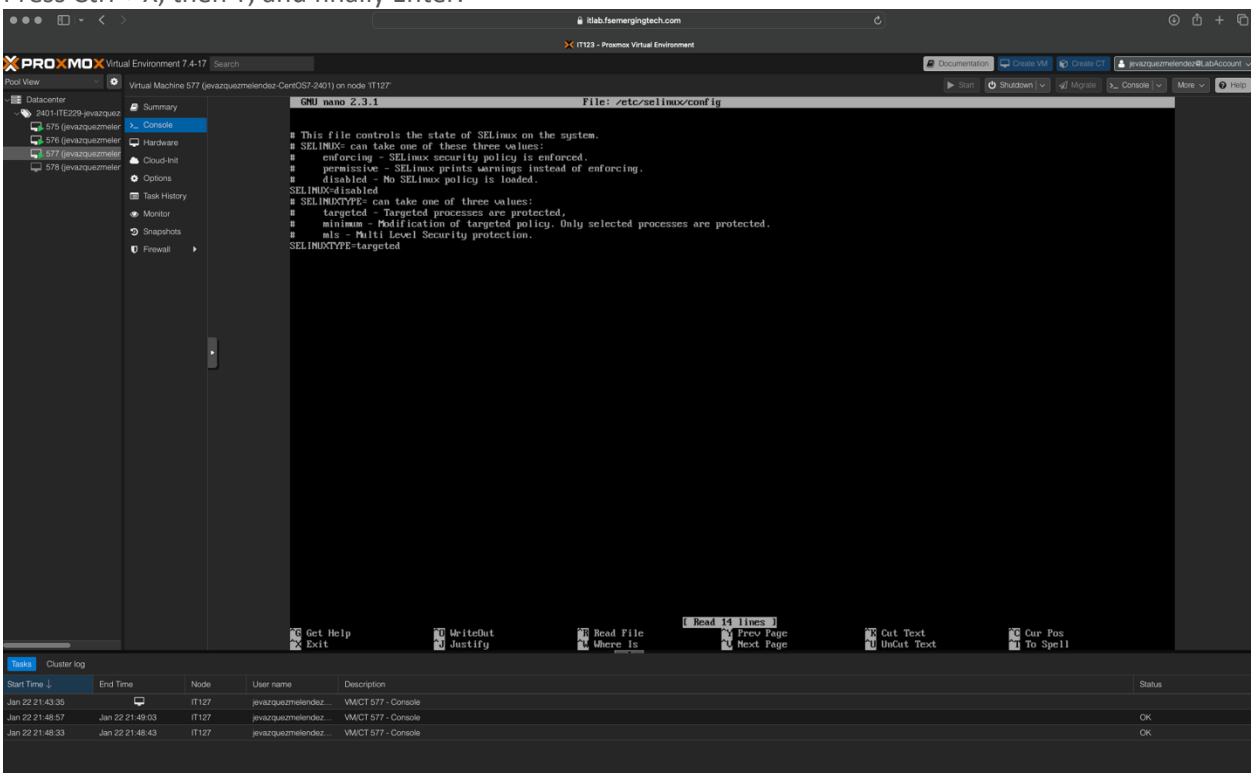


Test SELinux

sudo nano /etc/selinux/config

Locate the line that starts with SELINUX= and test if it remains disabled.

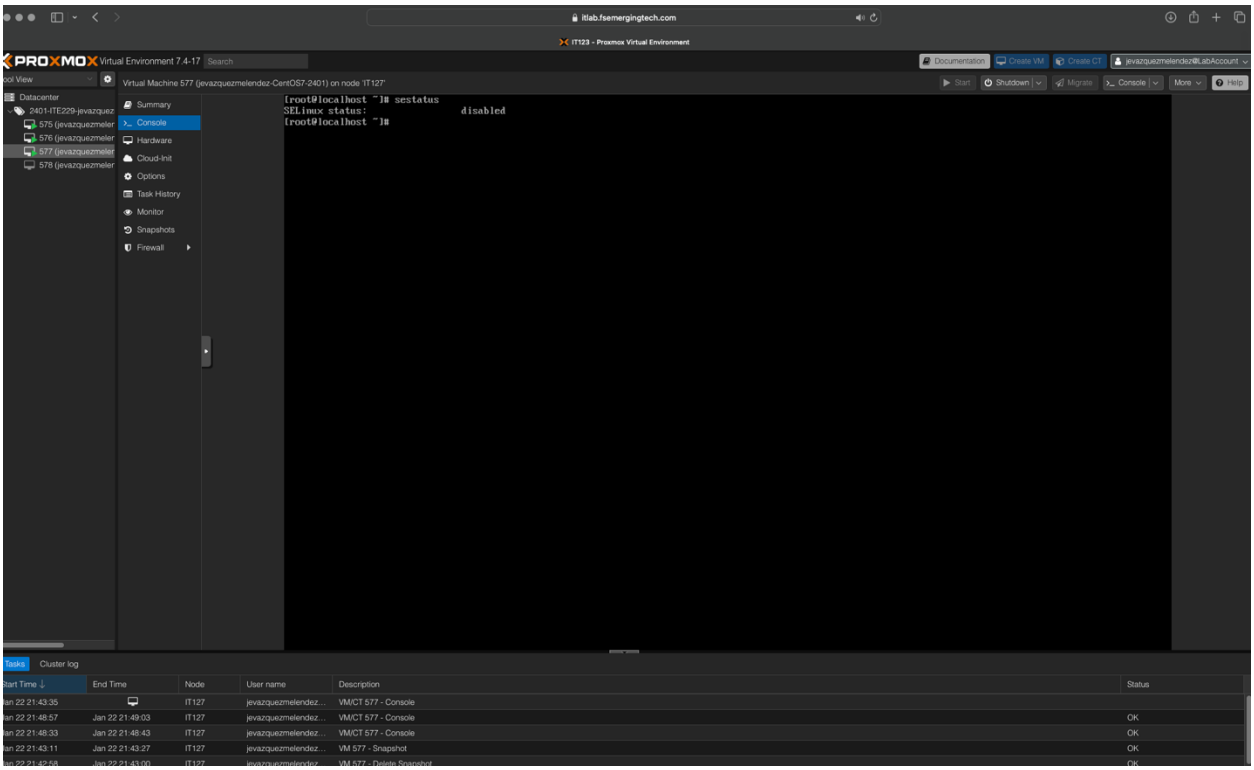
Press Ctrl + X, then Y, and finally Enter.



Confirm SELinux Status

sestatus

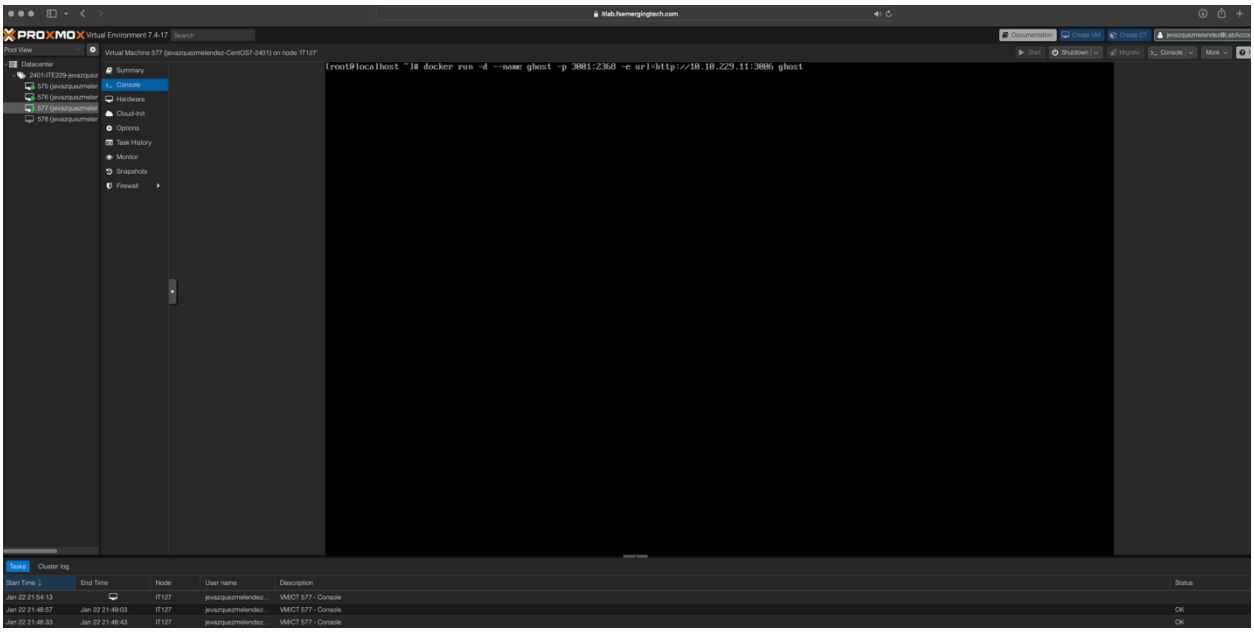
This command is used to check the status of the SELinux (Security-Enhanced Linux) system on a Linux machine.



Install Ghost Docker Container

docker run -d --name ghost -p 3001/2368 -e url=http///10.10.229.11/blog ghost

This command runs a containerized application called "ghost, " a blogging platform. The -d flag starts the container in detached mode, meaning it runs in the background. The --name flag is used to give the container a name, in this case, "ghost." The -p flag maps the host machine's port `3001` to the container's port `2368`. This is done so the blog can be accessed from the host machine's browser by going to http://localhost:3001/blog domain. The -e flag sets an environment variable called URL, which specifies the blog's URL. In this case, it is set to http://10.10.229.11/blog. Finally, "ghost" at the end of the command specifies the name of the Docker image for the container.

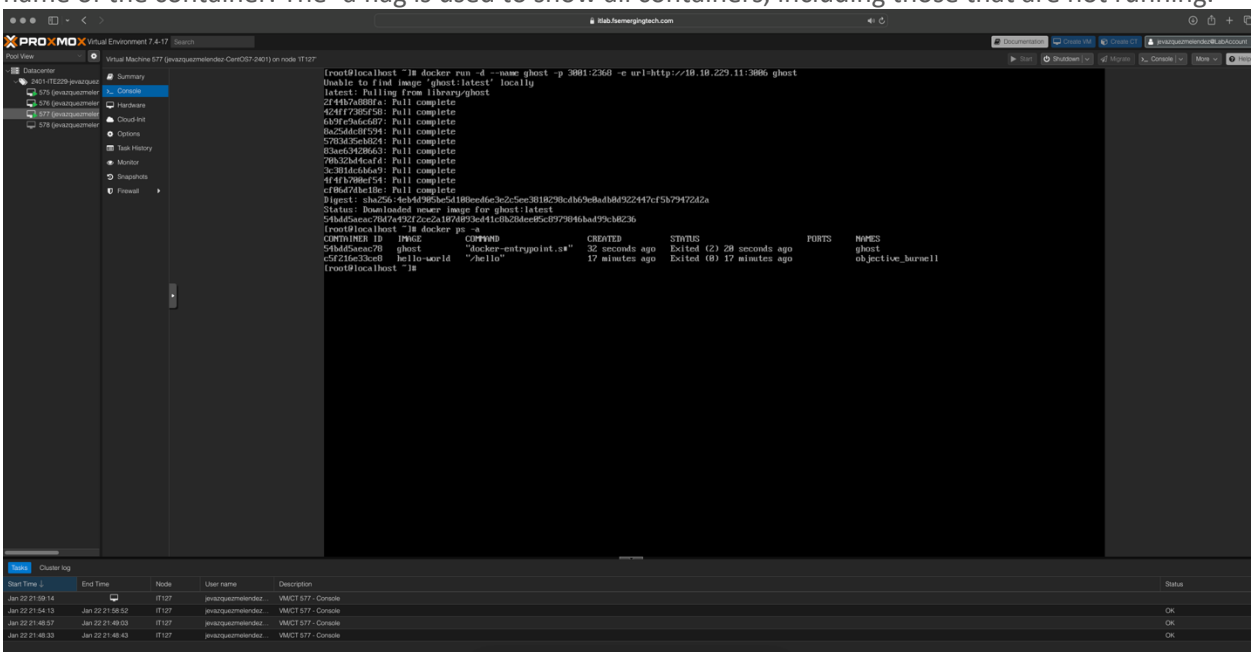


Test Ghost

Ghost Container ID

docker ps -a

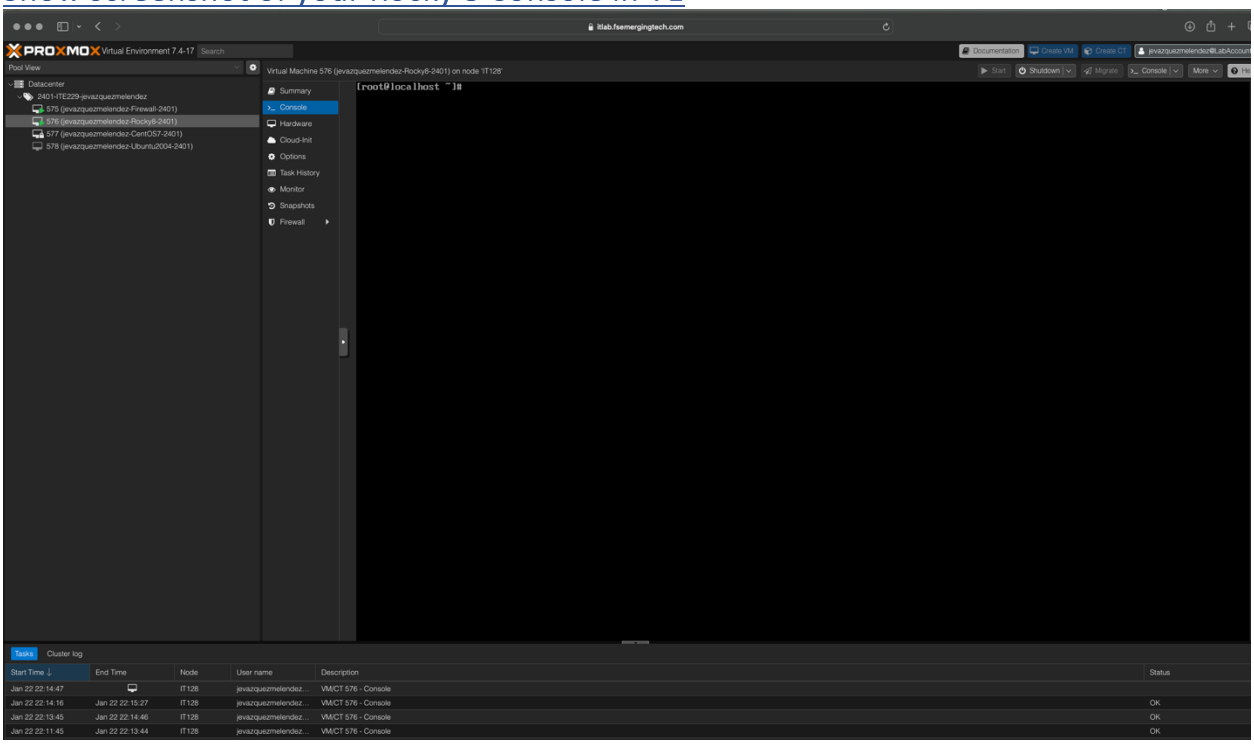
The command docker ps -a lists all the containers that have been created on the system, including their status, container ID, image used to create the container, command that was used, creation time, and name of the container. The -a flag is used to show all containers, including those that are not running.



IMPORTANT: To earn full credit, original formatting of this document must remain in place. In addition, ALL screenshots must include a “full view”, including your ProxMox title bar with your username showing.

Milestone #1: NginX Reverse Proxy

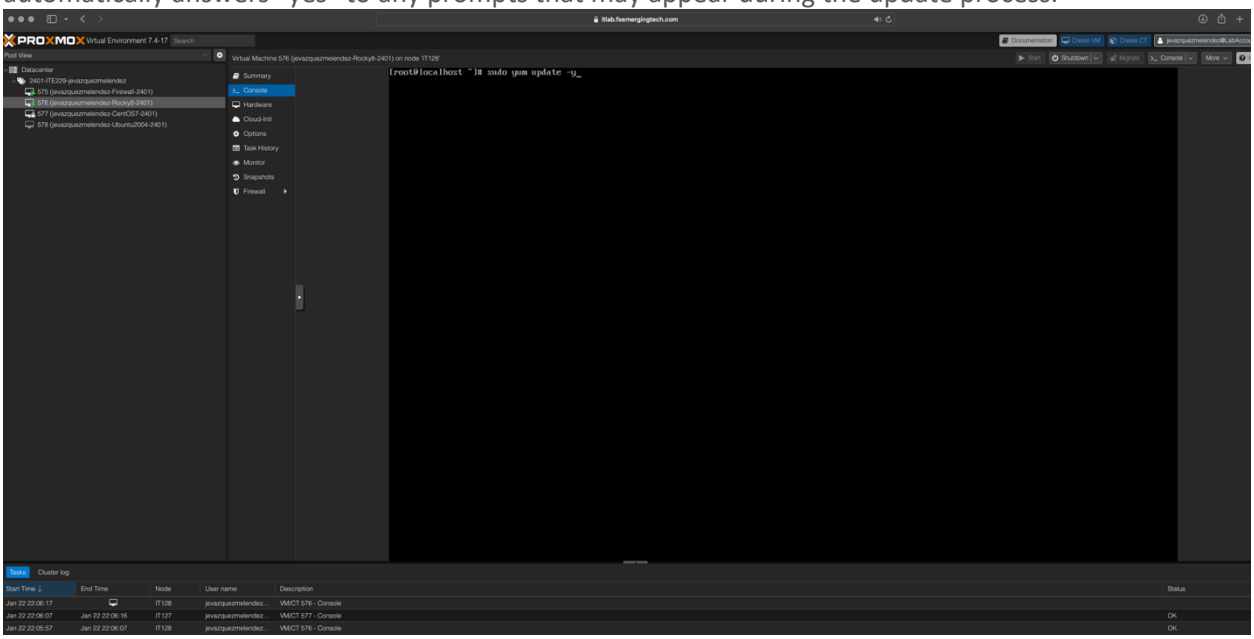
Show screenshot of your Rocky 8 Console in VE



Update Rocky 8

sudo yum update -y

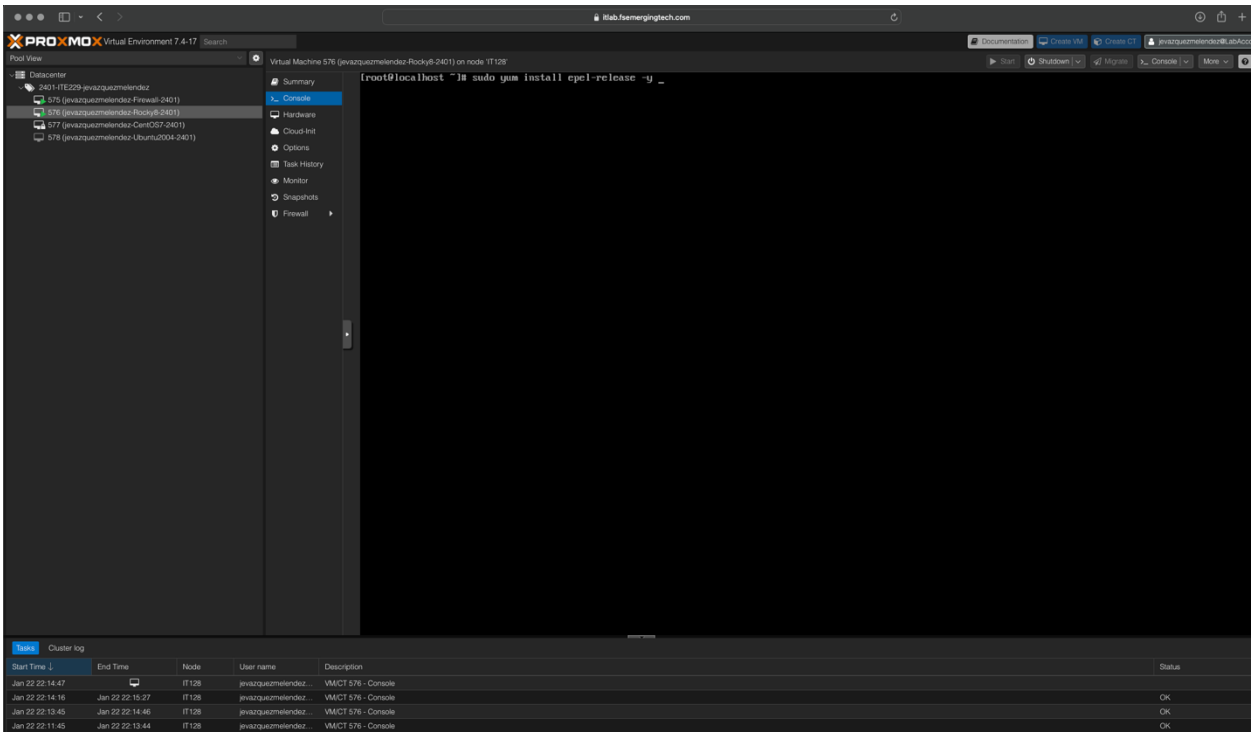
The command sudo yum update -y is used to update the installed packages on your system. The -y flag automatically answers "yes" to any prompts that may appear during the update process.



Install EPEL Packages

sudo yum install epel-release -y

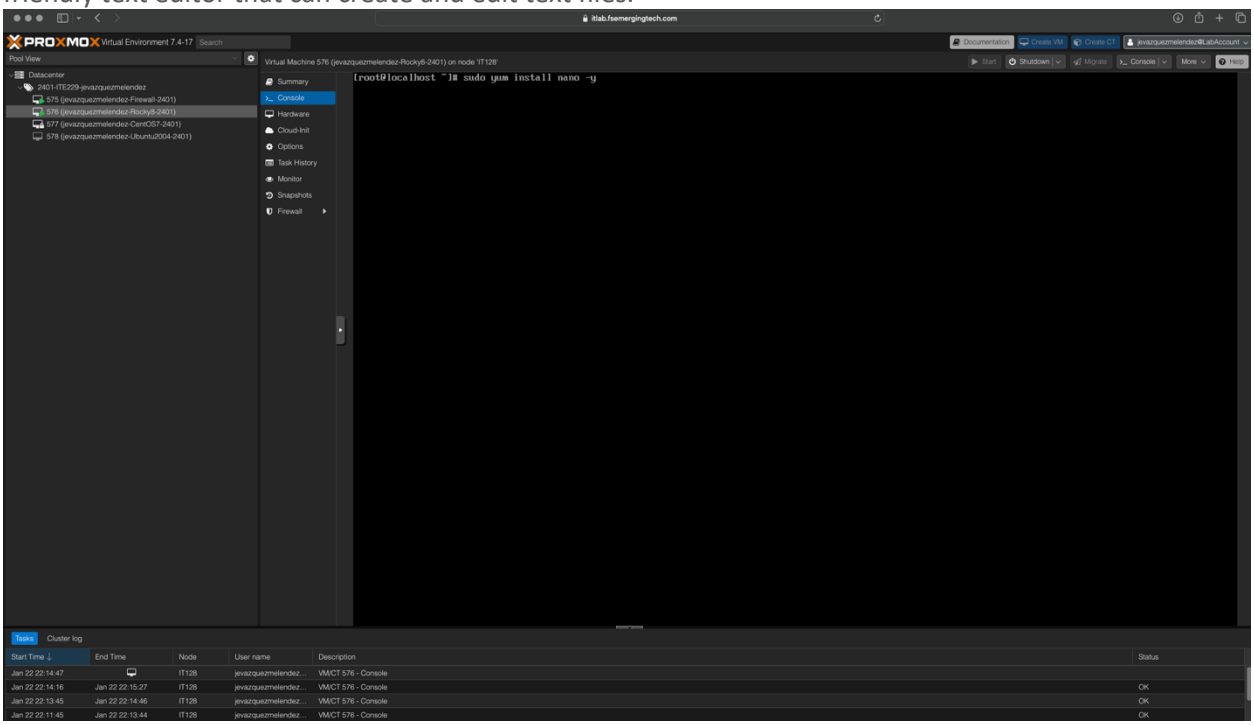
The command sudo yum install epel-release installs your system's Extra Packages for Enterprise Linux (EPEL) repository. This repository contains additional software packages not included in the default repositories provided by your Linux distribution.



Install Nano Editor

sudo yum install nano -y

The command sudo yum install nano installs the Nano text editor on your system. Nano is a simple, user-friendly text editor that can create and edit text files.



Disable SELinux

sudo nano /etc/selinux/config

To disable SELinux by editing its configuration file, you can follow these steps:

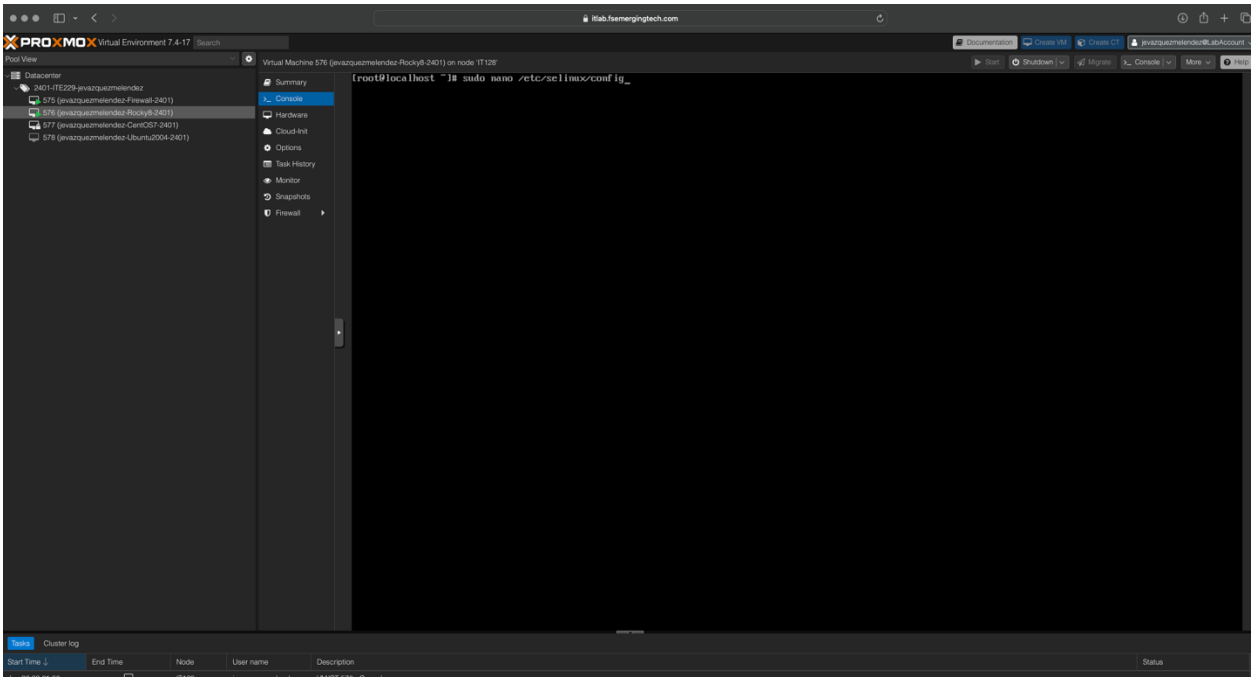
Run the following command to open the SELinux configuration file in the Nano text editor with root privileges:

sudo nano /etc/selinux/config

Locate the line that starts with SELINUX= and change its value to disabled.

Save the changes by pressing Ctrl + X and pressing enter.

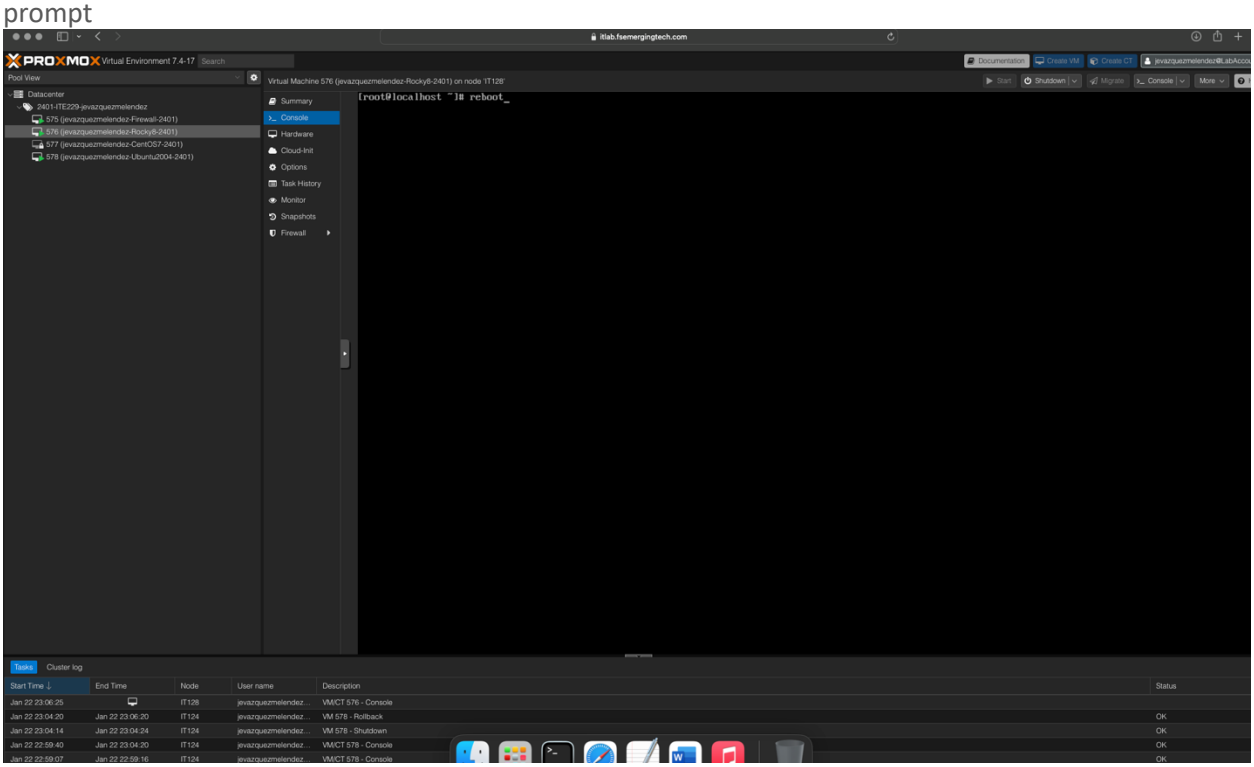
Reboot your system for the changes to take effect.



Reboot VM

reboot

This command is used to reboot or reset a Virtual Machine from the terminal shell using a command prompt



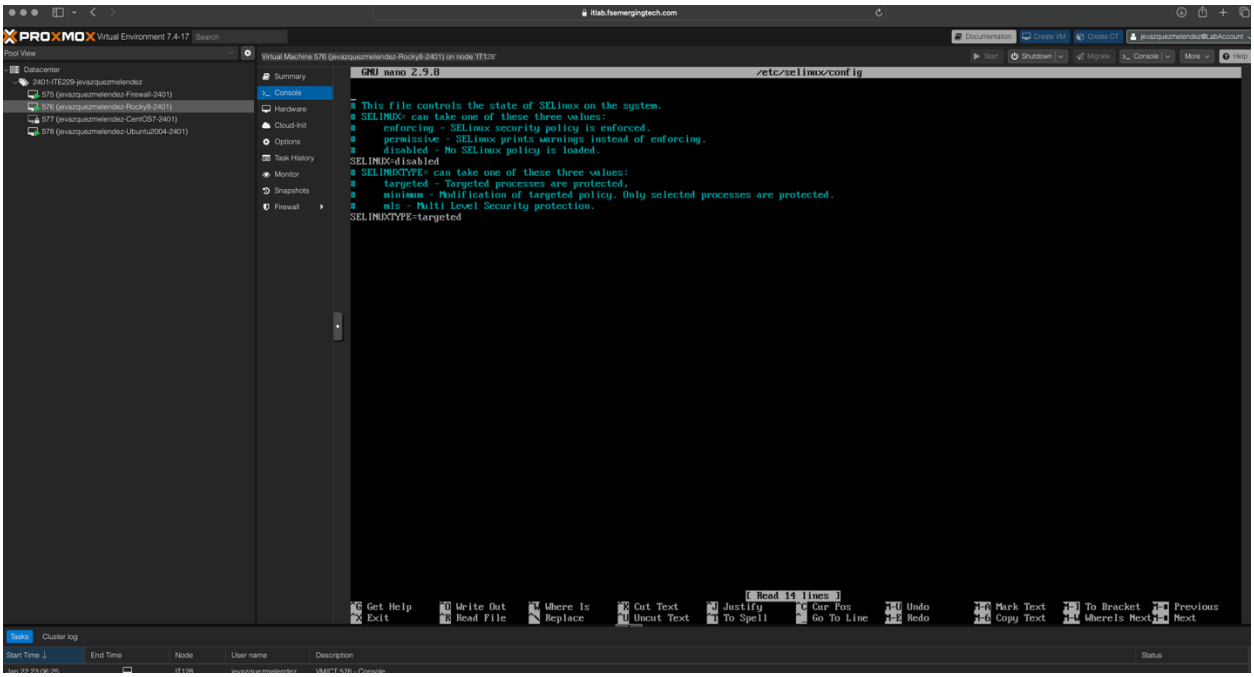
Test SELinux

sudo nano /etc/selinux/config

Locate the line that starts with SELINUX= and change its value to disabled.

Save the changes by pressing Ctrl + X and pressing enter.

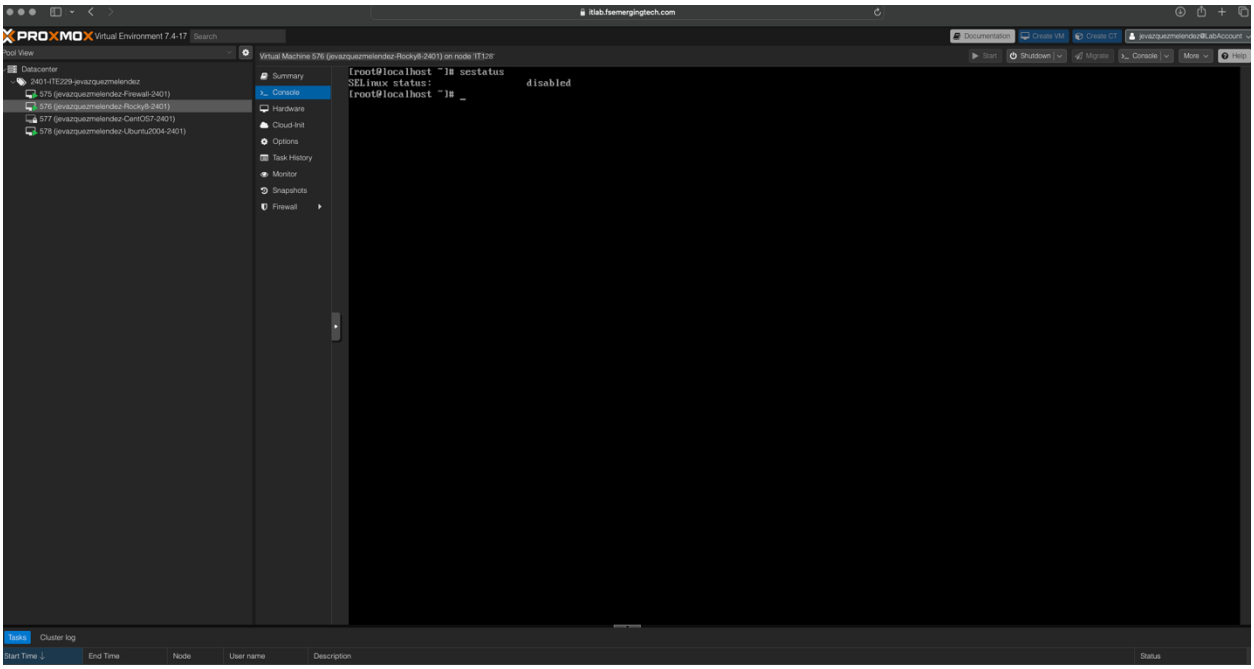
Reboot your system for the changes to take effect.



Confirm SELinux Status

sestatus

This command is used to check the status of the SELinux (Security-Enhanced Linux) system on a Linux machine.

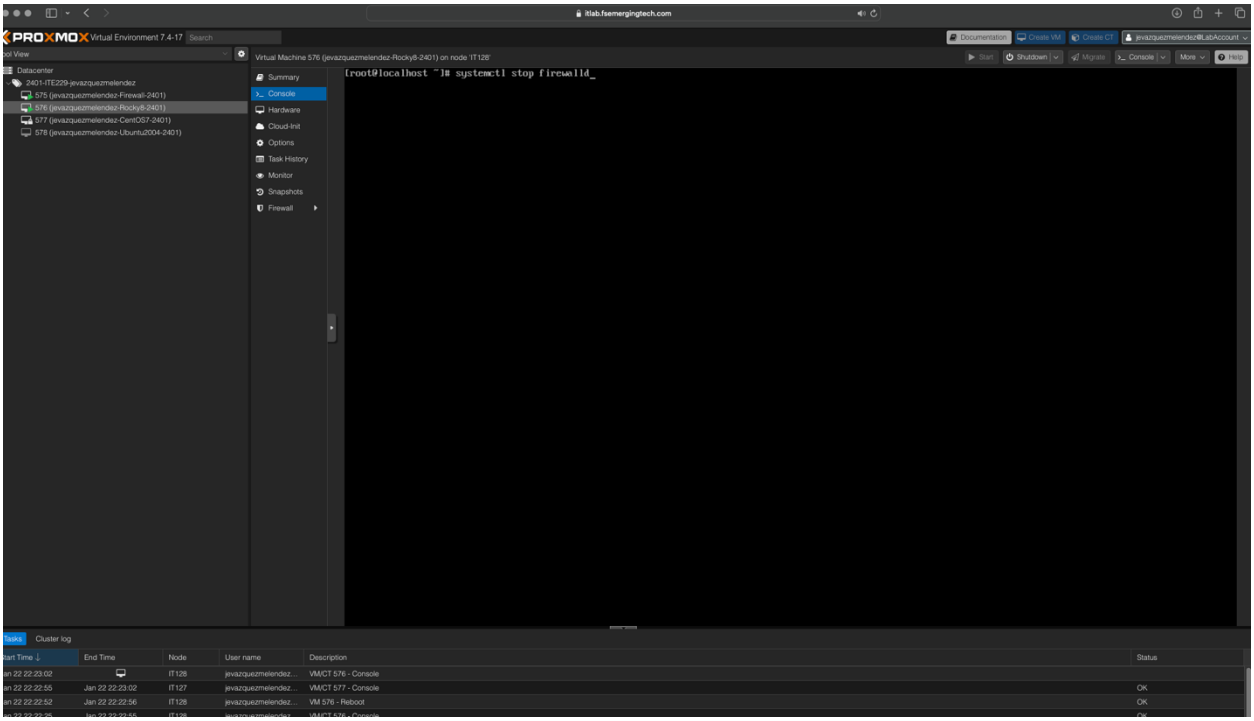


Rocky Firewall

Stop Firewall

systemctl stop firewalld

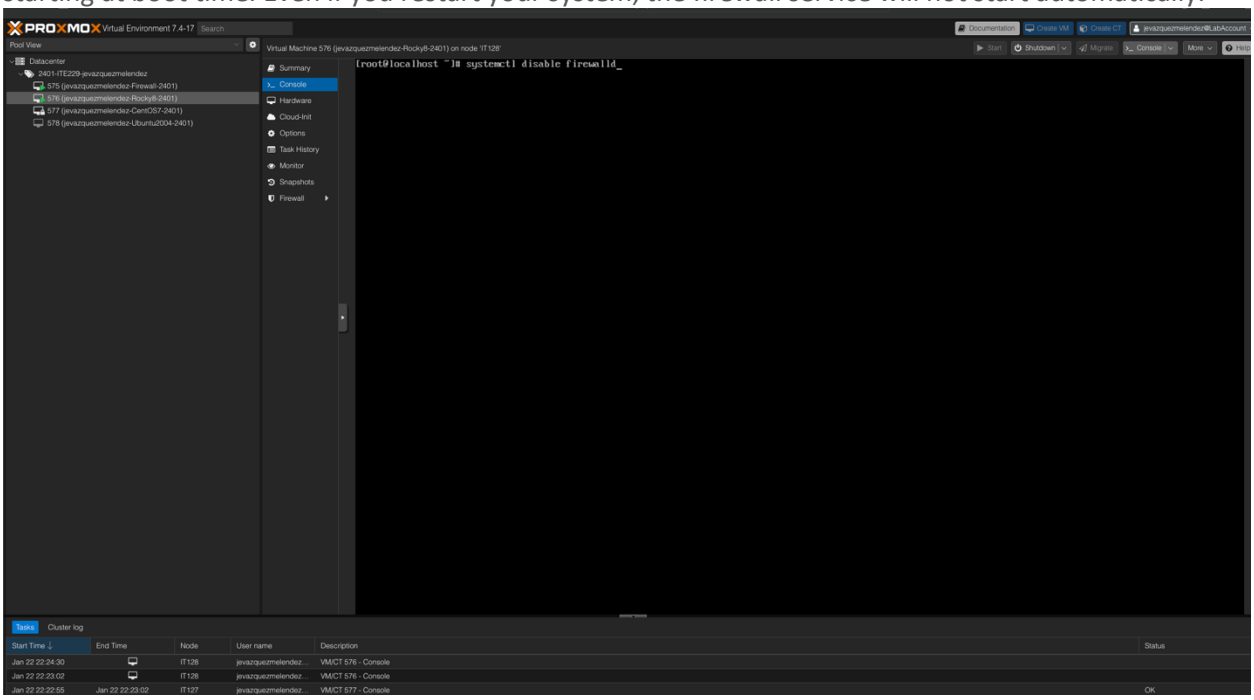
The systemctl stop firewalld command is used to stop the firewall service on your Linux system. When you stop the firewall service, all network traffic to and from your system will be allowed by default.



Disable Firewall

systemctl disable firewalld

On the other hand, the systemctl disable firewall command is used to prevent the firewall service from starting at boot time. Even if you restart your system, the firewall service will not start automatically.

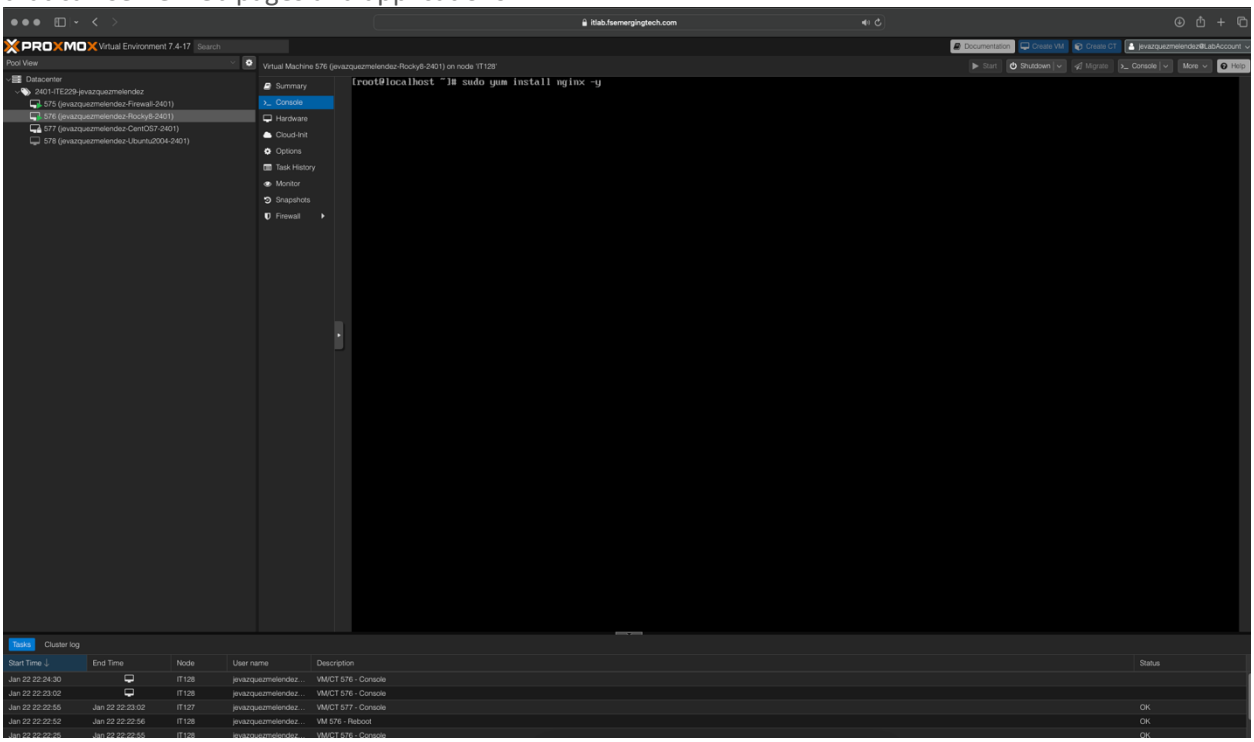


NginX

Install NginX

sudo yum install nginx -y

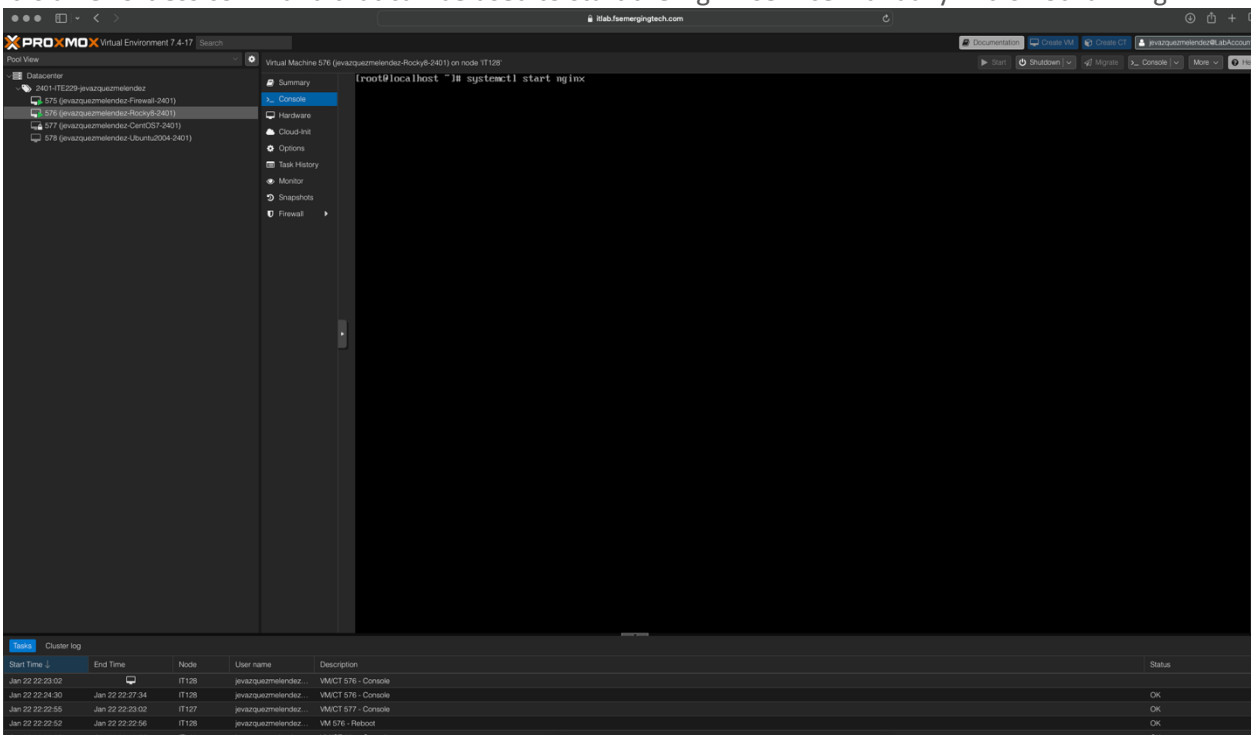
This command installs the Nginx web server on the system. Nginx is a popular open-source web server that can serve web pages and applications



Start NginX

systemctl start nginx

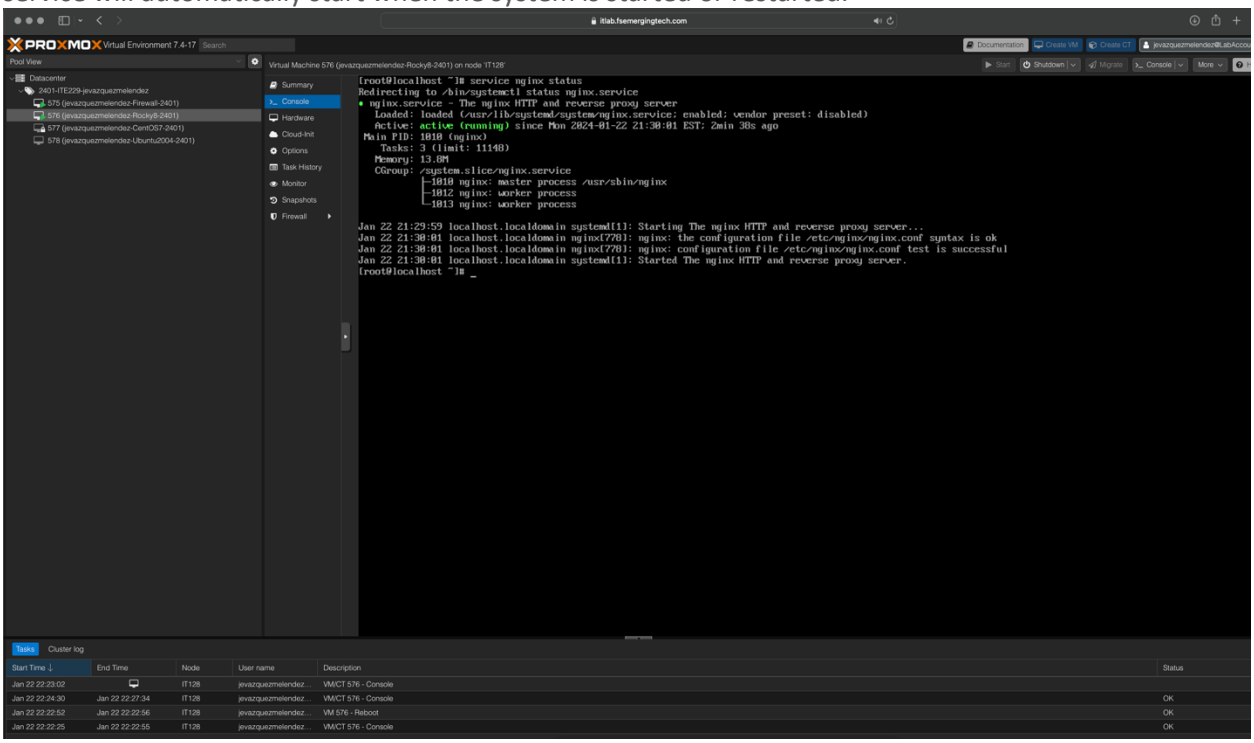
This command starts the Nginx web server service on your Linux system.
This command initiates the Nginx service, and the web server will start serving web pages and applications.
It is an effortless command that can be used to start the Nginx service manually if it is not running.



Enable NginX

systemctl enable nginx

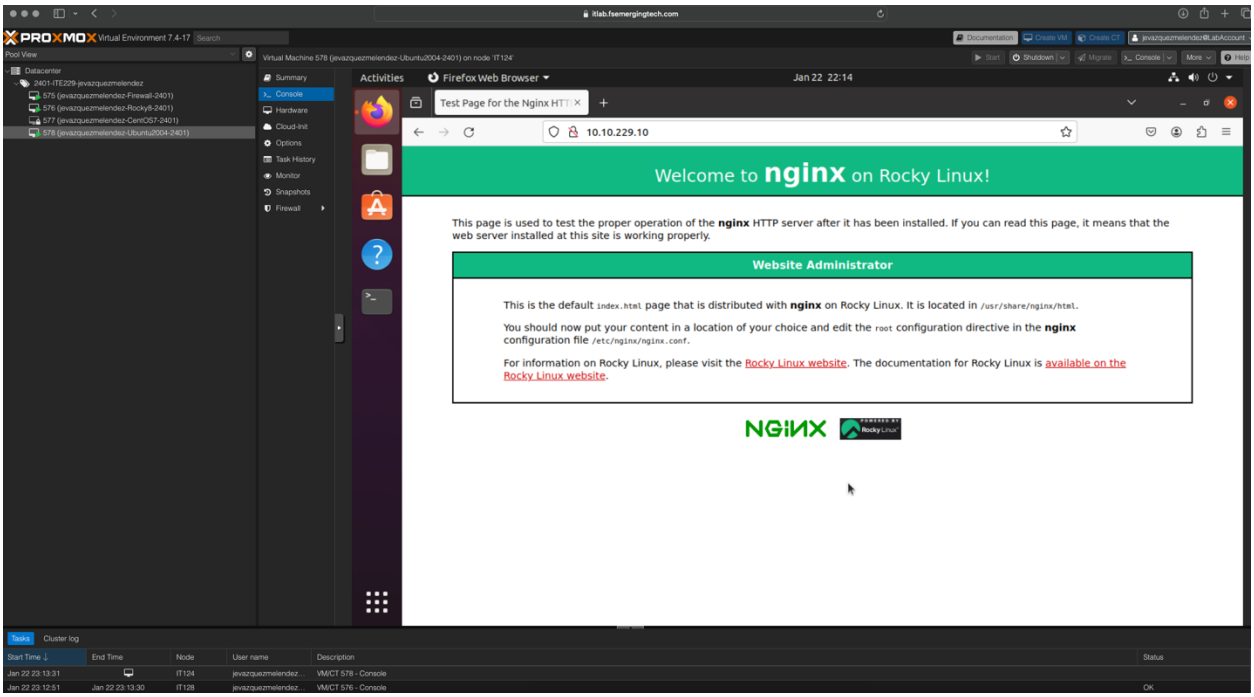
This command enables the Nginx service to start automatically at boot time. This means the Nginx service will automatically start when the system is started or restarted.



Test NginX

This command starts the Nginx web server service on your Linux system. This command initiates the Nginx service, and the web server will start serving web pages and applications. It is an effortless command that can be used to start the Nginx service manually if it is not running.

To test a Nginx server with a Ghost Docker container running on a specific IP address (let's say IP address 10.10.229.10, you can use a web browser to access the IP address of the Nginx server from the Ubuntu VM. If the Nginx server is appropriately configured to proxy requests to the Ghost container, you should see the Ghost blog's homepage when accessing the IP address of the Nginx server through the web browser.

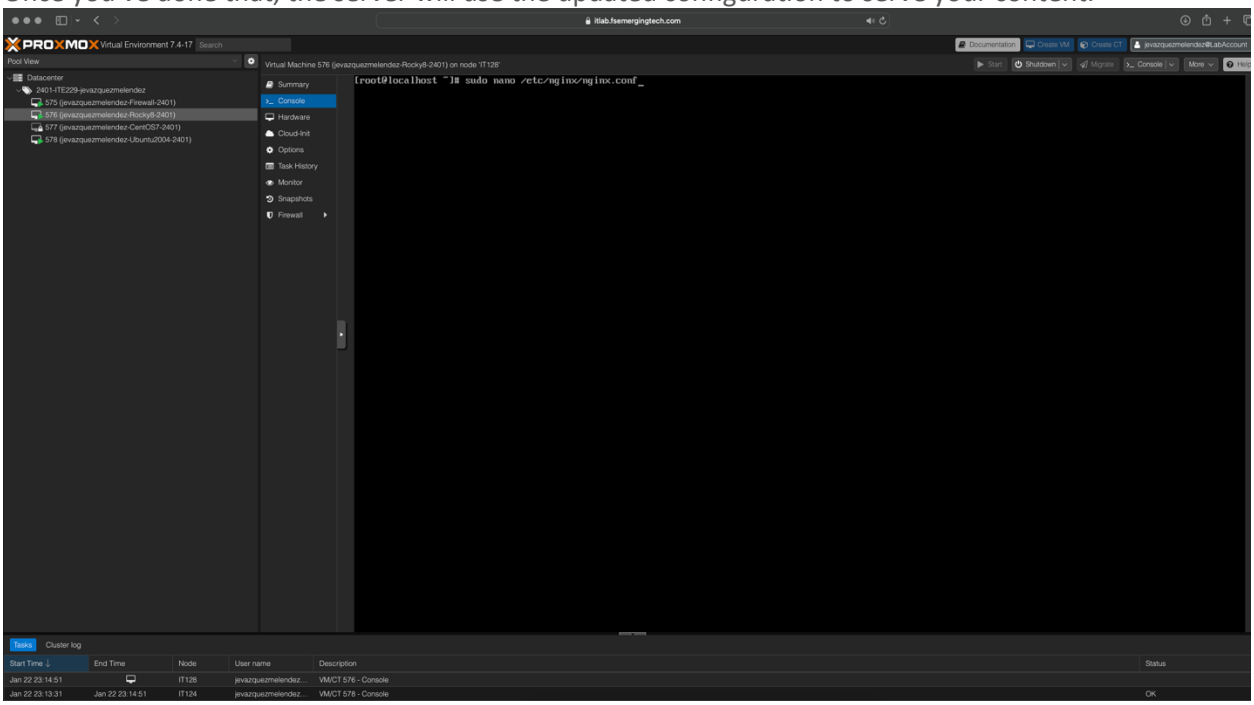


Reverse Proxy for Ghost Site

Edit NginX configuration file

sudo nano /etc/ngnix/nginx.conf

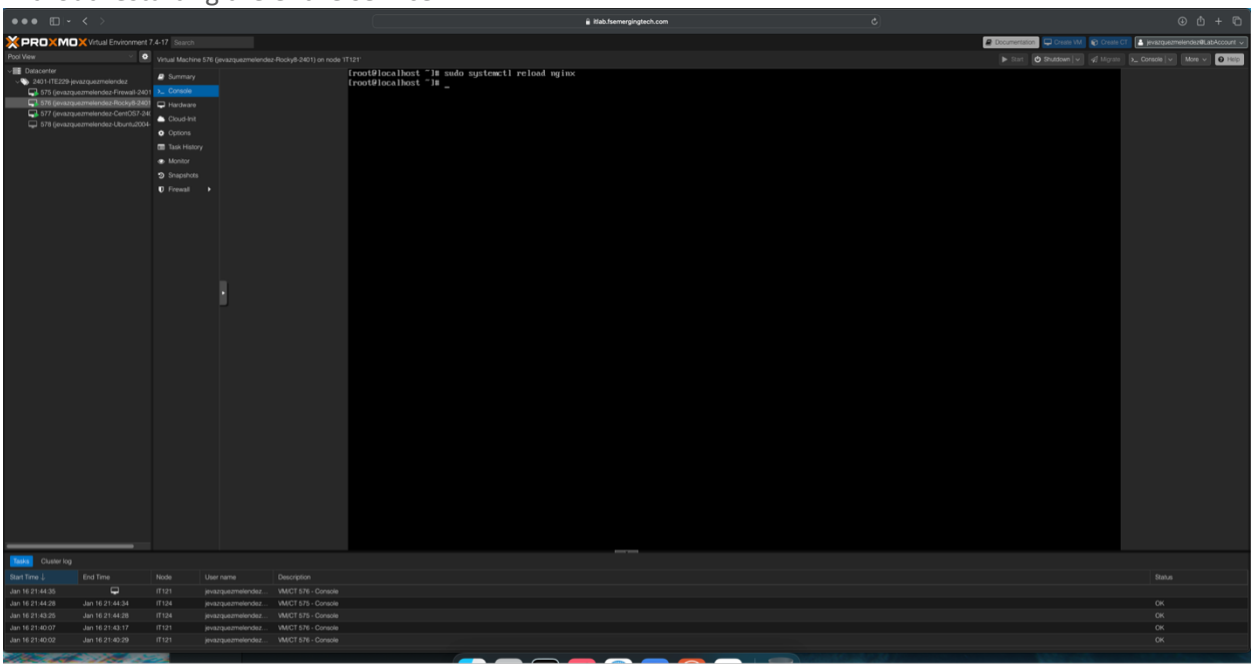
Editing the Nginx configuration file is a way to make changes to the settings of a web server, such as Ghost. Modifying this file allows you to adjust the server's behavior, performance, security, and more. The process involves opening the file, finding the relevant section, making changes, and saving the file. Once you've done that, the server will use the updated configuration to serve your content.



Reload NginX service

sudo systemctl reload nginx

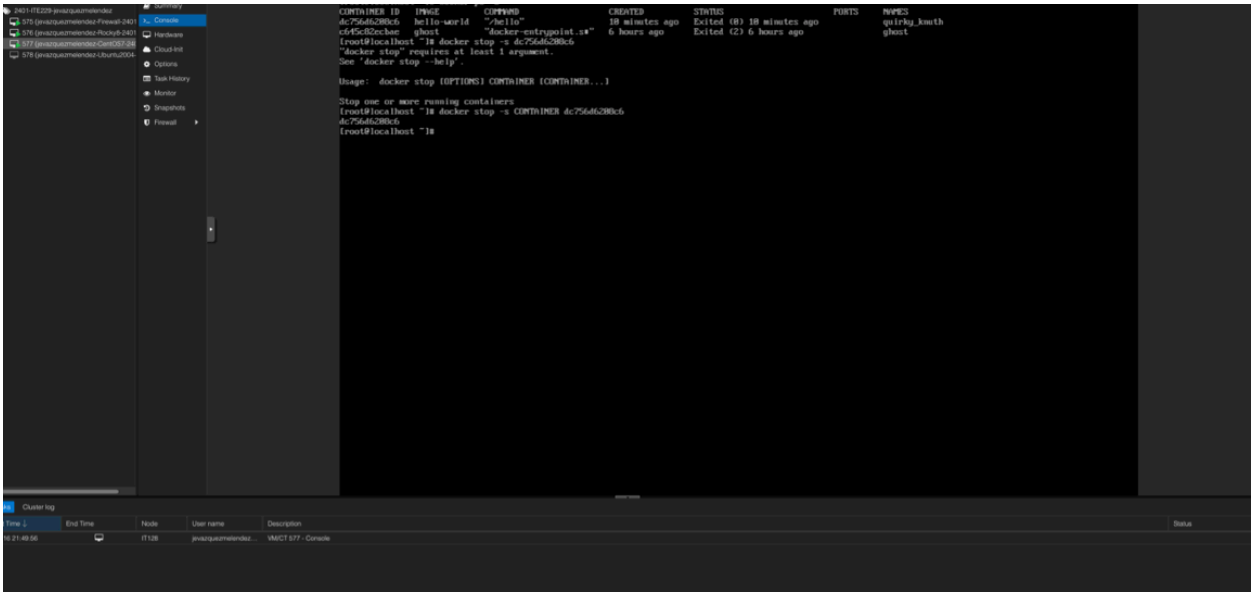
The command you entered will reload the configuration of the nginx service using sudo privileges. This is useful if you have made changes to the nginx configuration files and want those changes to take effect without restarting the entire service.



Terminate Docker

docker stop -s CONTAINER [CONTAINER-ID]

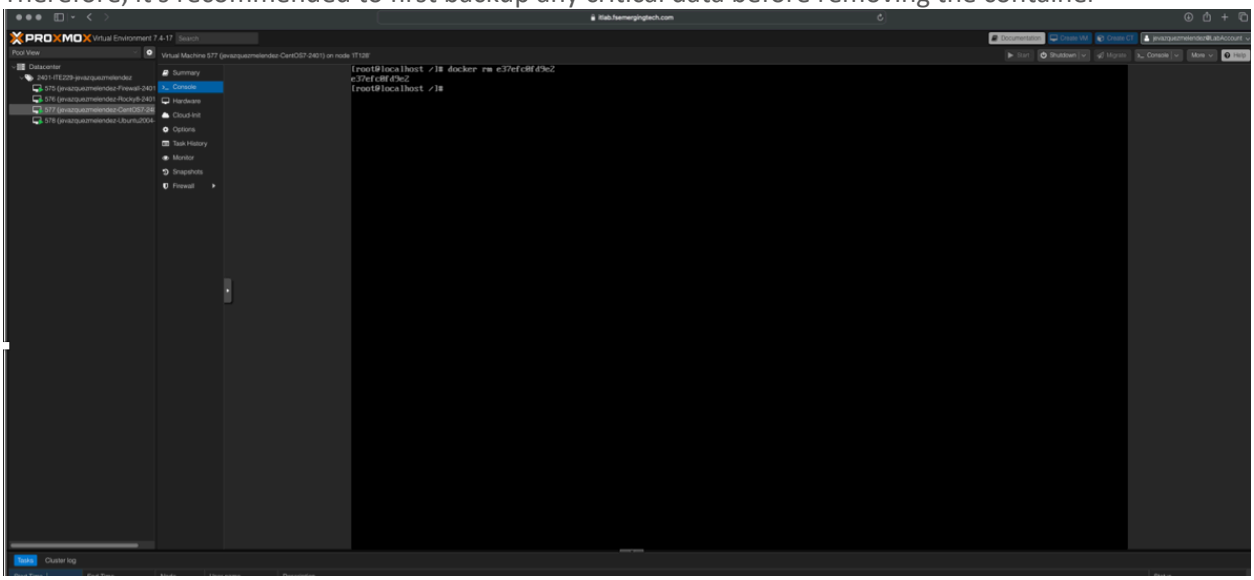
This command stops a running Docker container. The "-s" option is used to specify the signal to be sent to the container when it is stopped. In this case, "CONTAINER" is just a placeholder for the actual name or ID of the container that needs to be stopped. So, when this command is executed, the specified container will be gracefully stopped, and all the processes running inside the container will be terminated.



Delete Ghost Container

docker rm [CONTAINER-ID]

The "docker rm [CONTAINER-ID]" command removes a stopped or running Docker container. The "[CONTAINER-ID]" part of the command should be replaced with the actual ID of the container that you want to remove. If the specified container runs, the command will stop it before removing it. It's important to note that any data or changes made inside the container will be lost after the container is removed. Therefore, it's recommended to first backup any critical data before removing the container



Create New Ghost Container

docker run -d --name ghost -p 3001:2368 -e url=http://10.10.229.10/blog ghost

This command is used in Docker, a popular software platform for creating and managing virtual containers.

The command "docker run" is used to start a new container.
In this case, the container is named "ghost".

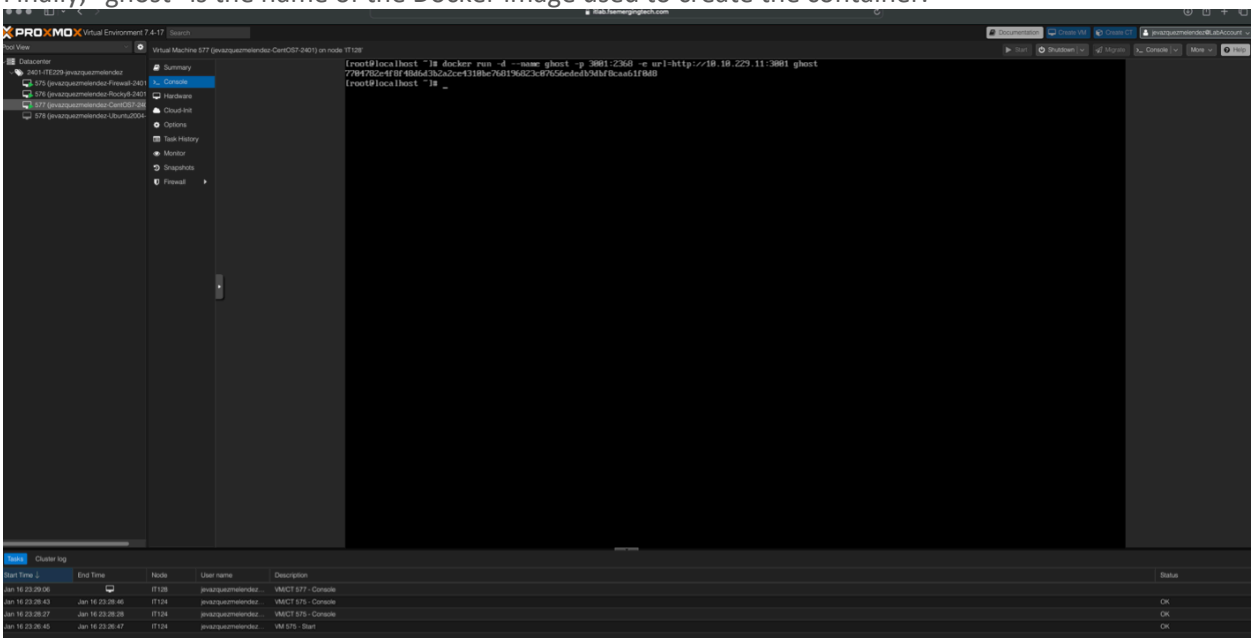
The "-d" flag runs the container in the background as a daemon.

The "--name" flag gives the container a specific name, in this case, "ghost."

The "-p" flag maps a port between the container and the host. It maps port 2368 in the container to port 3001 on the host computer.

The "-e" flag is used to set an environment variable. In this case, the environment variable "url" is set to http://10.10.229.10/blog.

Finally, "ghost" is the name of the Docker image used to create the container.

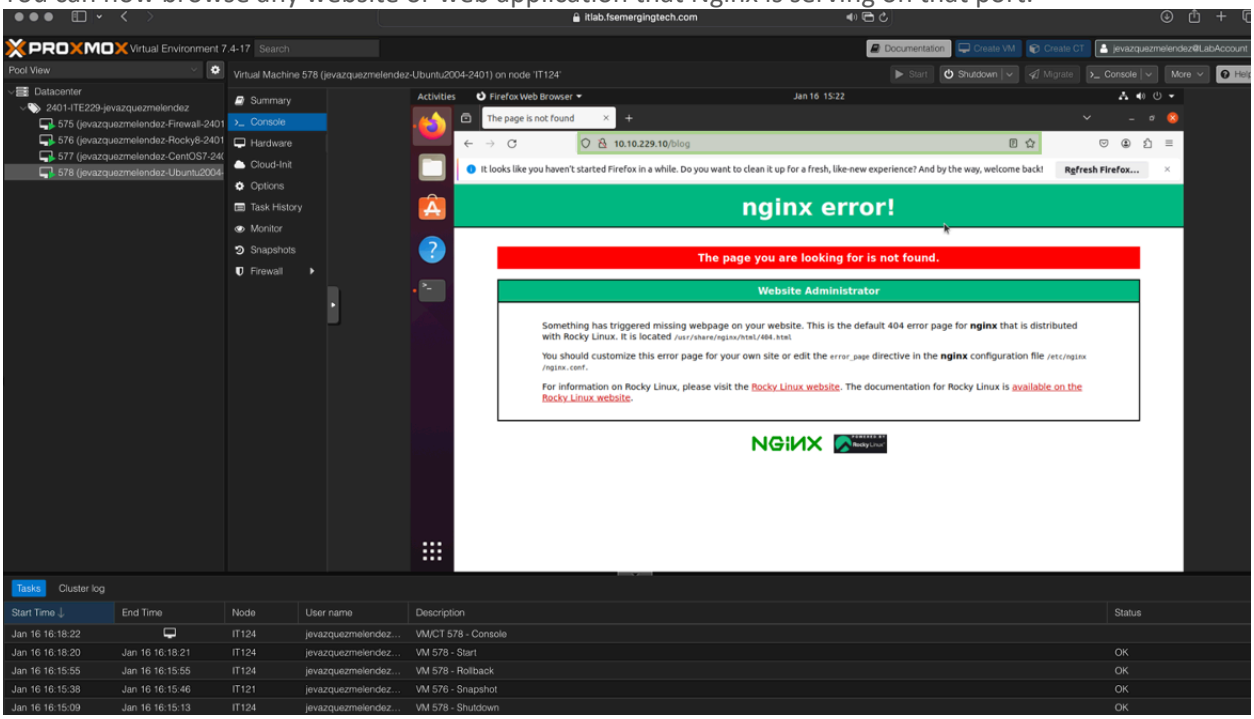


Browse to Ghost

To browse Nginx from an Ubuntu machine in simple terms, you can follow these steps:
Open a web browser on your Ubuntu machine.

In the address bar, type the IP address or hostname of the server where Nginx is running.
http://10.10.229.10

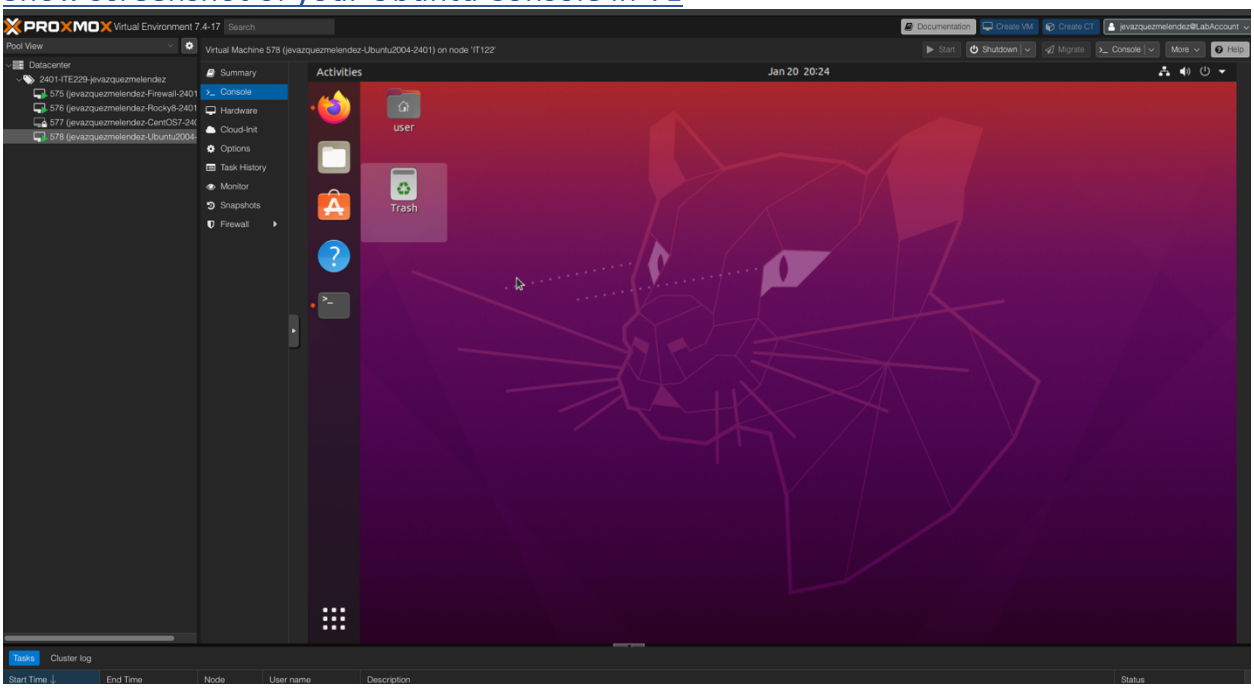
You can now browse any website or web application that Nginx is serving on that port.



IMPORTANT: To earn full credit, original formatting of this document must remain in place. In addition, ALL screenshots must include a “full view”, including your ProxMox title bar with your username showing.

Milestone #2: WordPress on Ubuntu - LAMP Stack

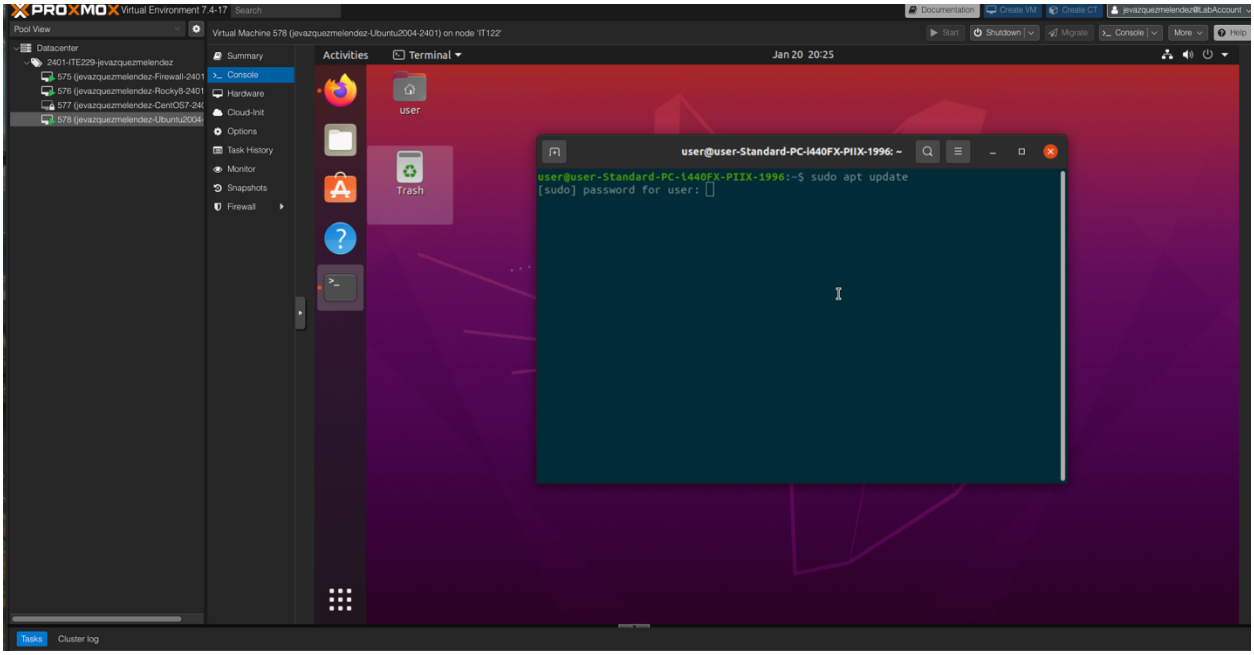
Show screenshot of your Ubuntu Console in VE



Update Ubuntu

$ sudo apt update -y

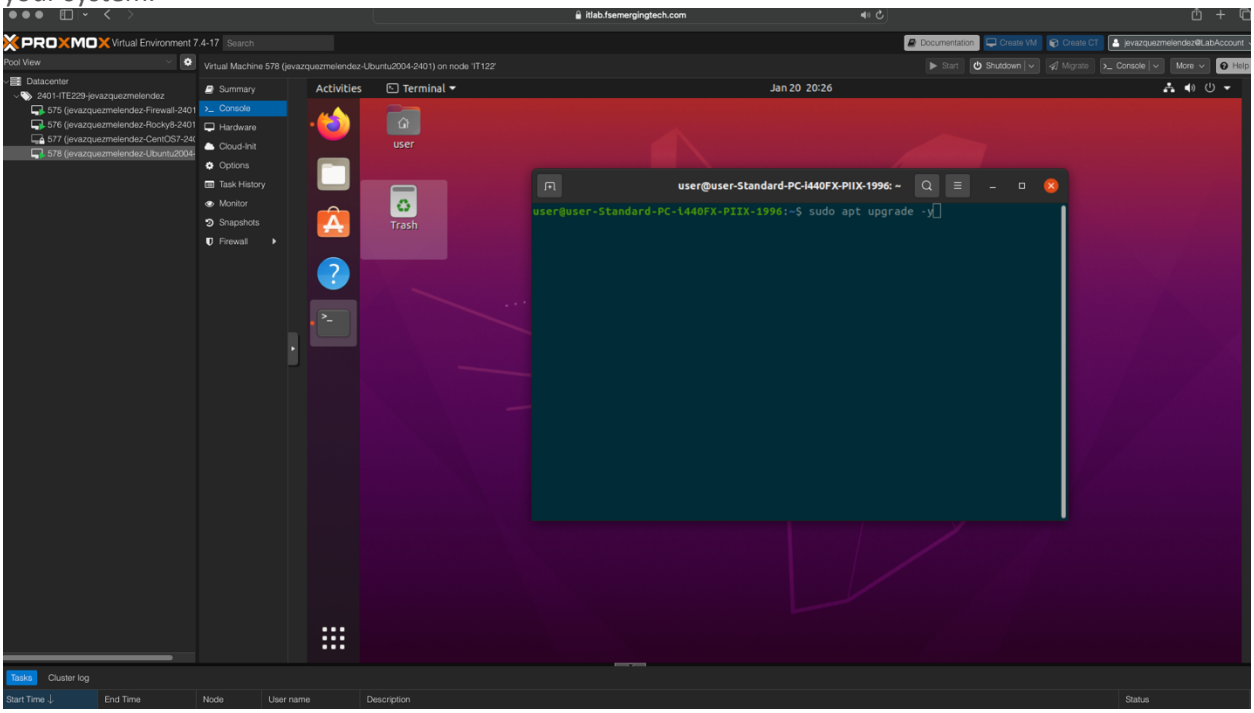
This command is used to update the list of available software packages from the internet on your Ubuntu system.



Upgrade Ubuntu

$ sudo apt upgrade -y

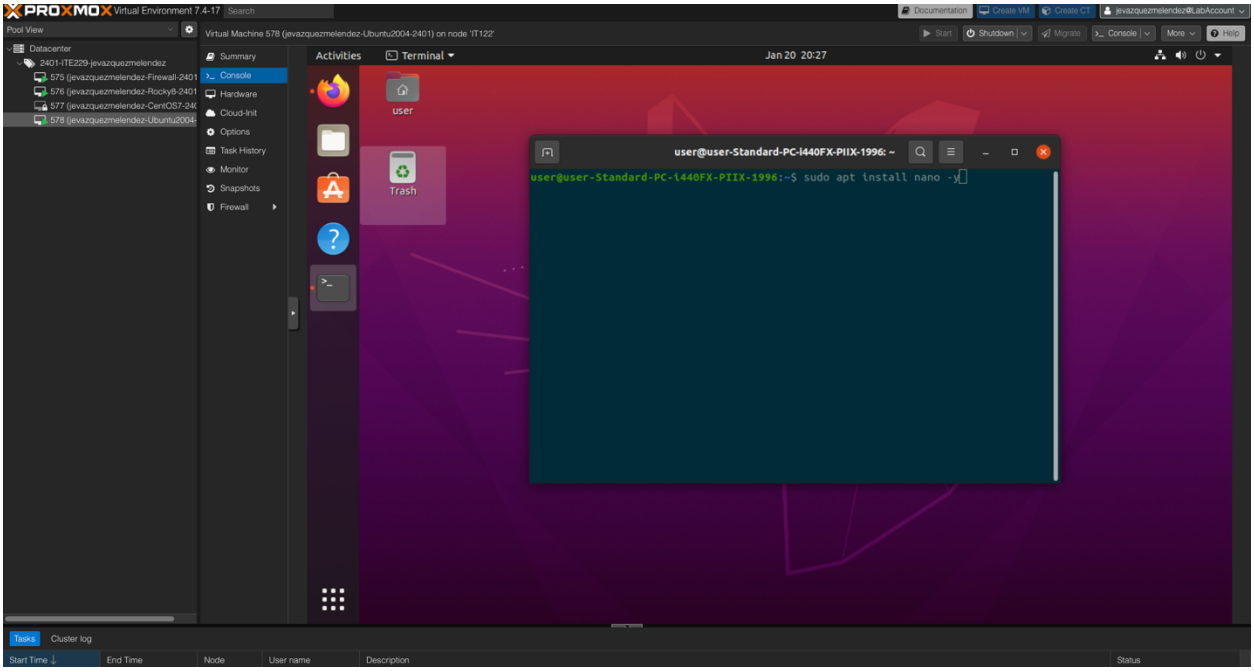
This command is used to download and install any available updates for the installed software packages on your system.



Install Nano Editor

$ sudo apt install nano -y

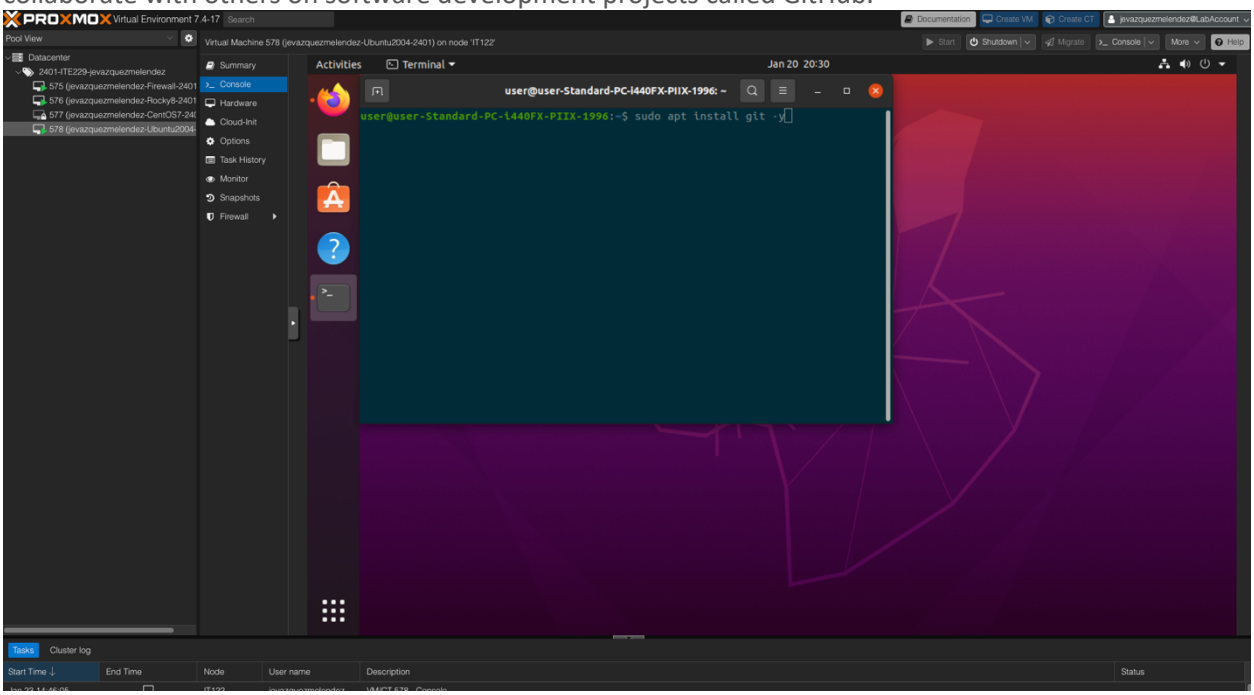
This command is used to install a text editor called 'nano' on your Ubuntu system, which can be used to modify files.



Install Git

$ sudo apt install git -y

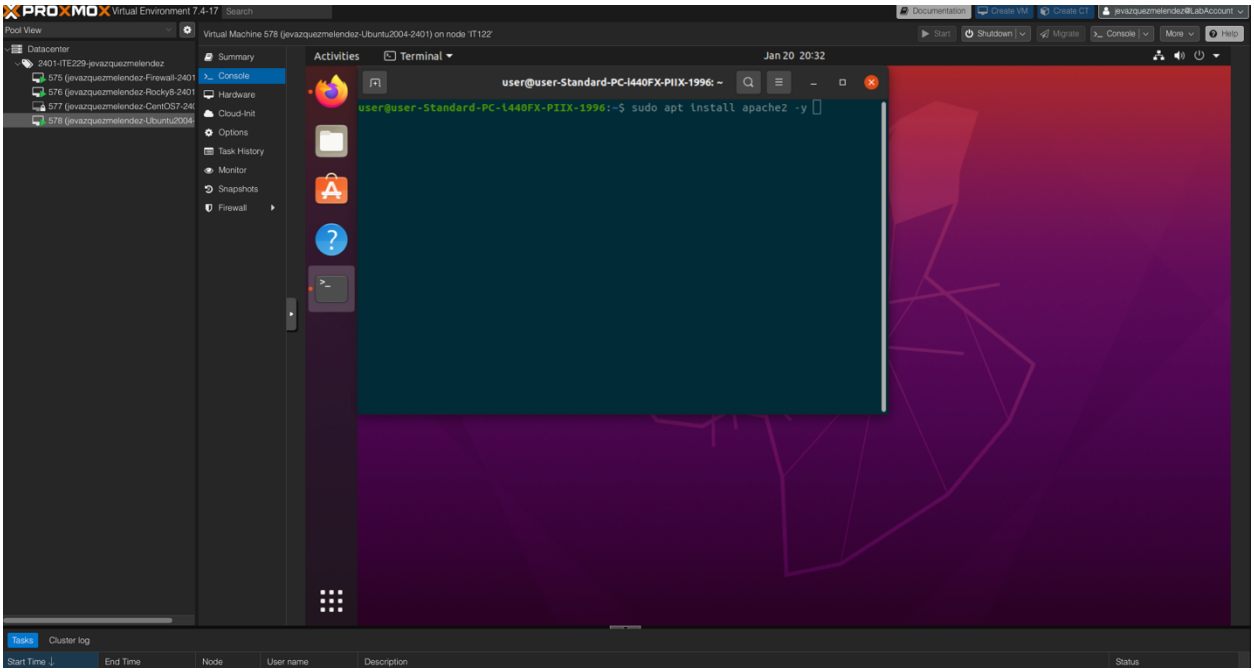
This command is used to install Git, a version control system that allows you to track changes in files and collaborate with others on software development projects called GitHub.



Install Apache2

$ sudo apt install apache2 -y

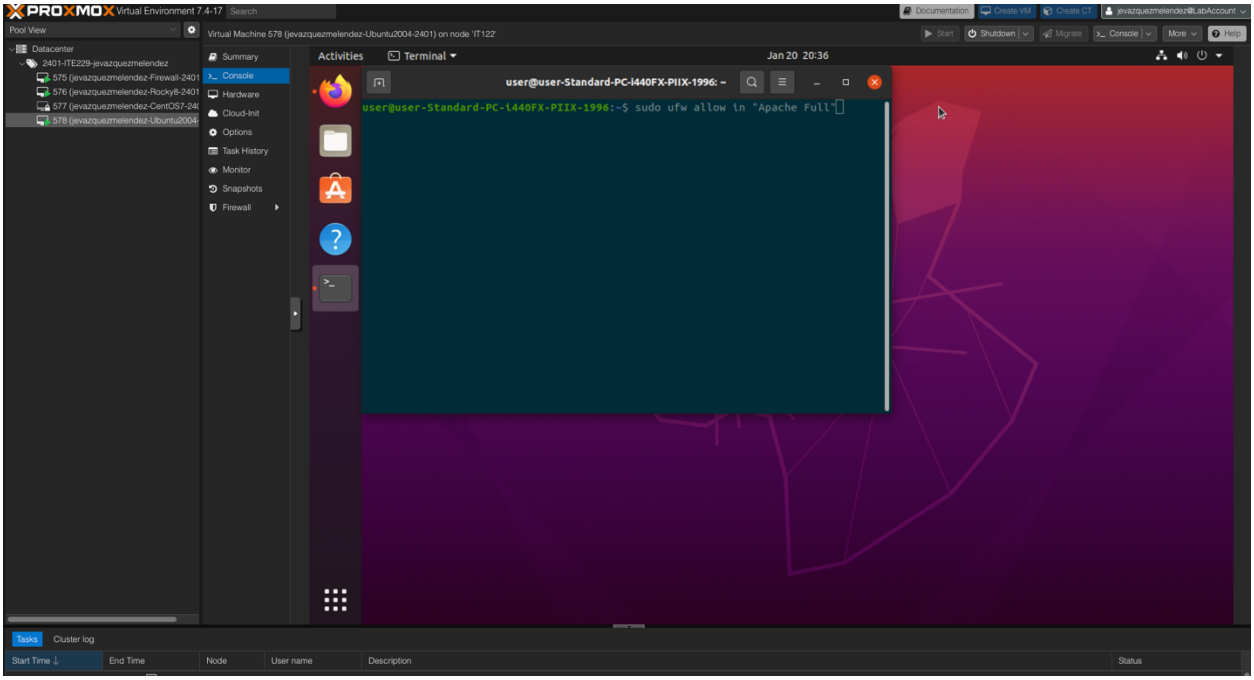
The command sudo apt install apache2 is used to install the Apache web server on your Ubuntu machine. This will allow you to host the proyect website or web application on your computer or virtal machine.



Open Firewall Ports 80 and 443

$ sudo ufw allow in “Apache Full”

The command is used to allow incoming traffic to your Apache web server through the firewall. This is important because by default, the firewall blocks all incoming traffic to your computer. The 'Apache Full' option allows access to both HTTP and HTTPS traffic.

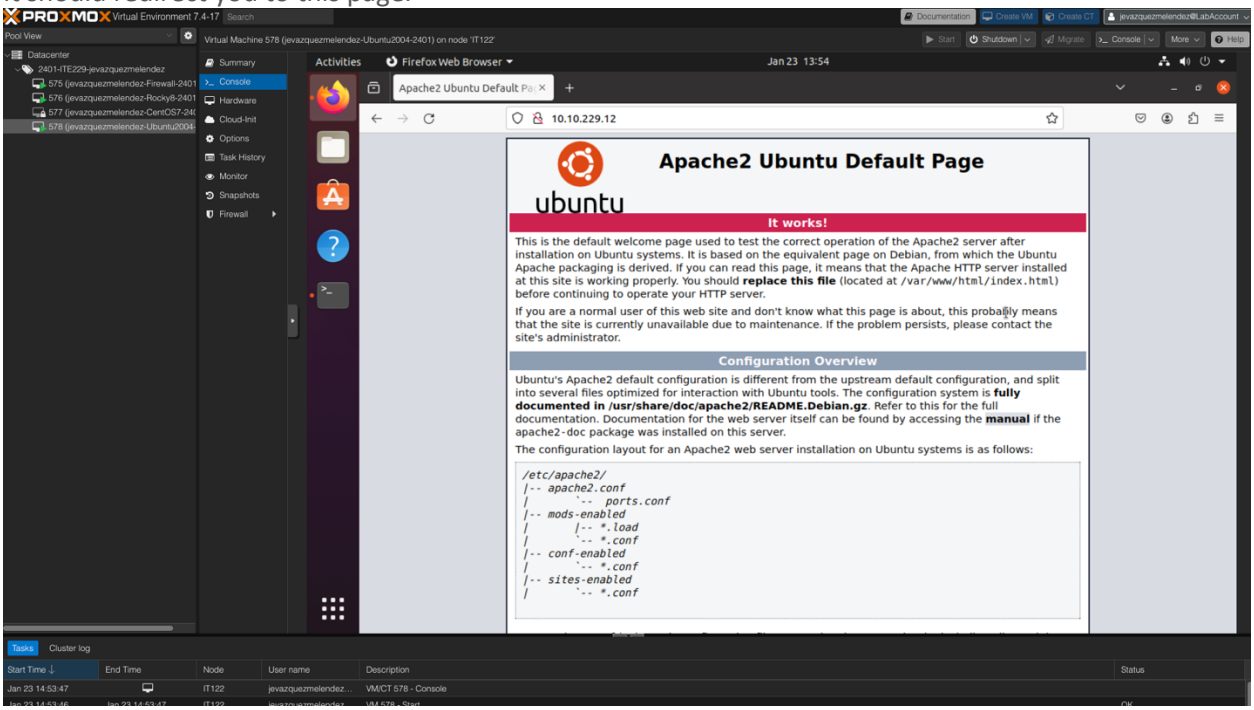


Browse to Apache2 Ubuntu Default Page

To Browser to the Apache2 Ubuntu Default Page you are going to open the Firefox Web Browser and Type:

http://10.10.229.12

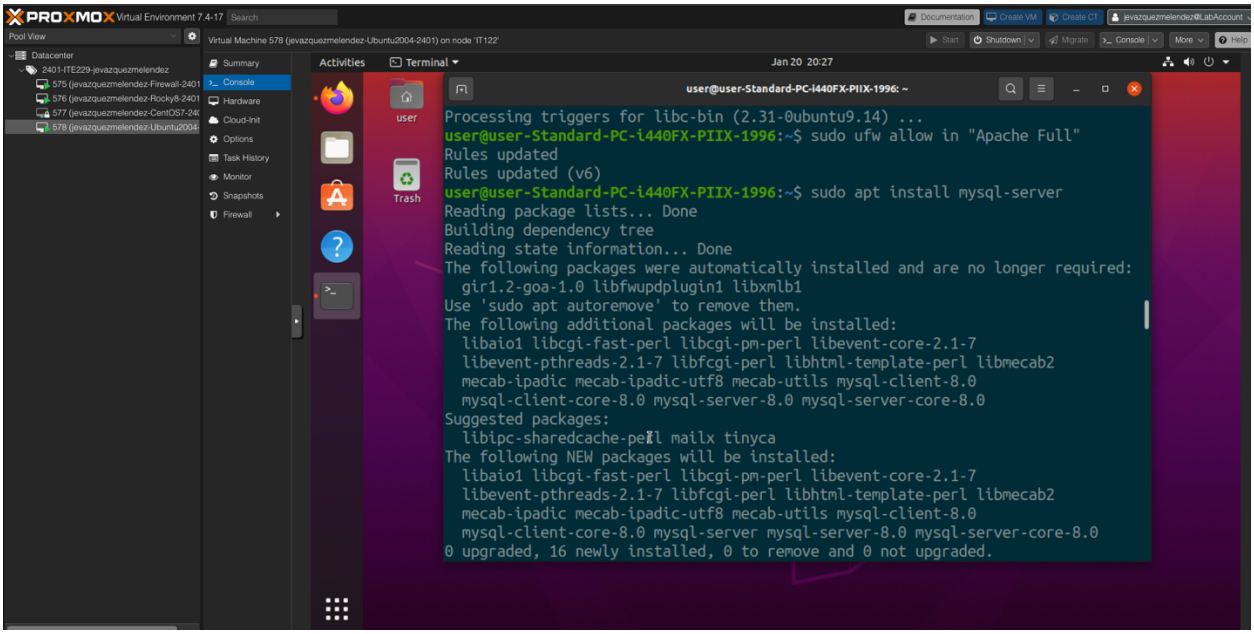
It should redirect you to this page.



Install MySQL

$ sudo apt install mysql-server

This comman allows you to install he first command, install the MySQL database server on your computer or virtual machine.



Alter root user password

TDJFid34c935kg59DR

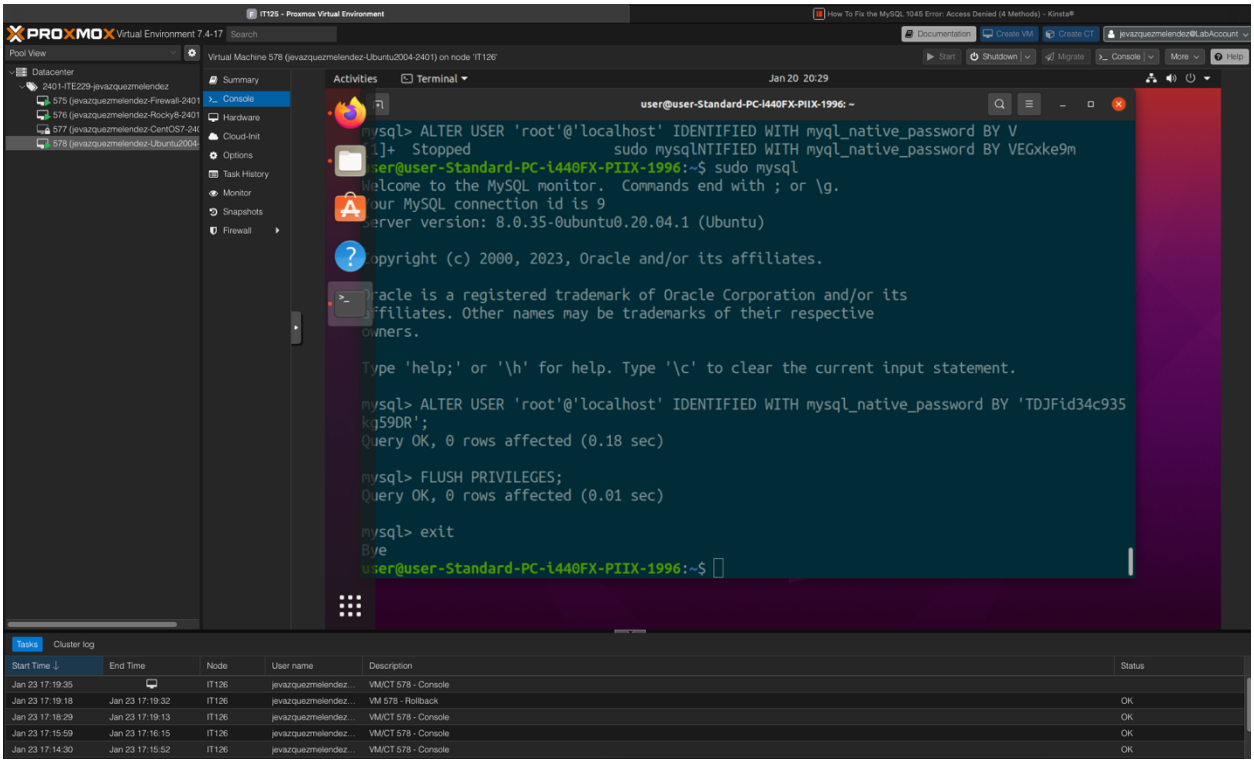
$ sudo myslq

This allows you to run the mysql command as the root user, which grants you more permissions and access to the MySQL server using the sudo priviliges.

Then to Alter root user password type the following command:

mysql> ALTER USER ‘root’@’localhost’ IDENTIFIED WITH mysql_native_password BY ‘TDJFid34c935kg59DR’;

Then Press Enter.

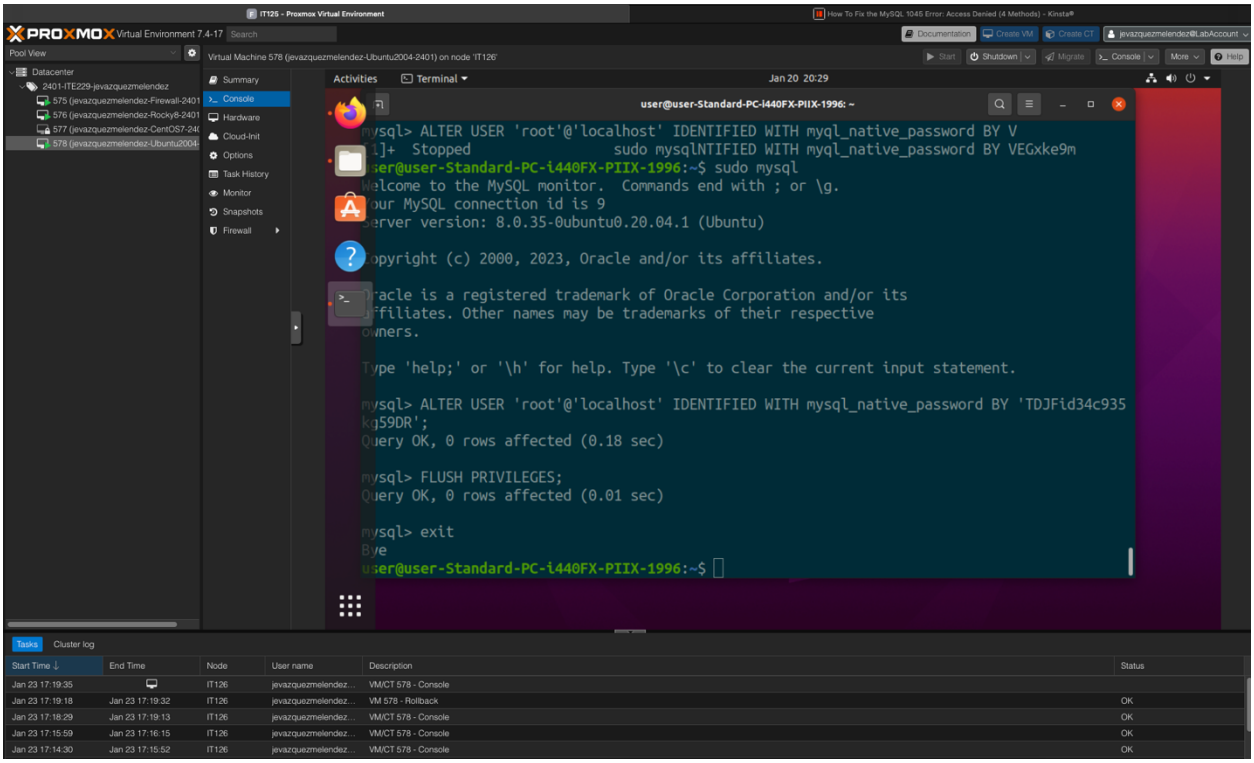


Flush Privileges

mysql> FLUSH PRIVILEGES;

Press Enter.

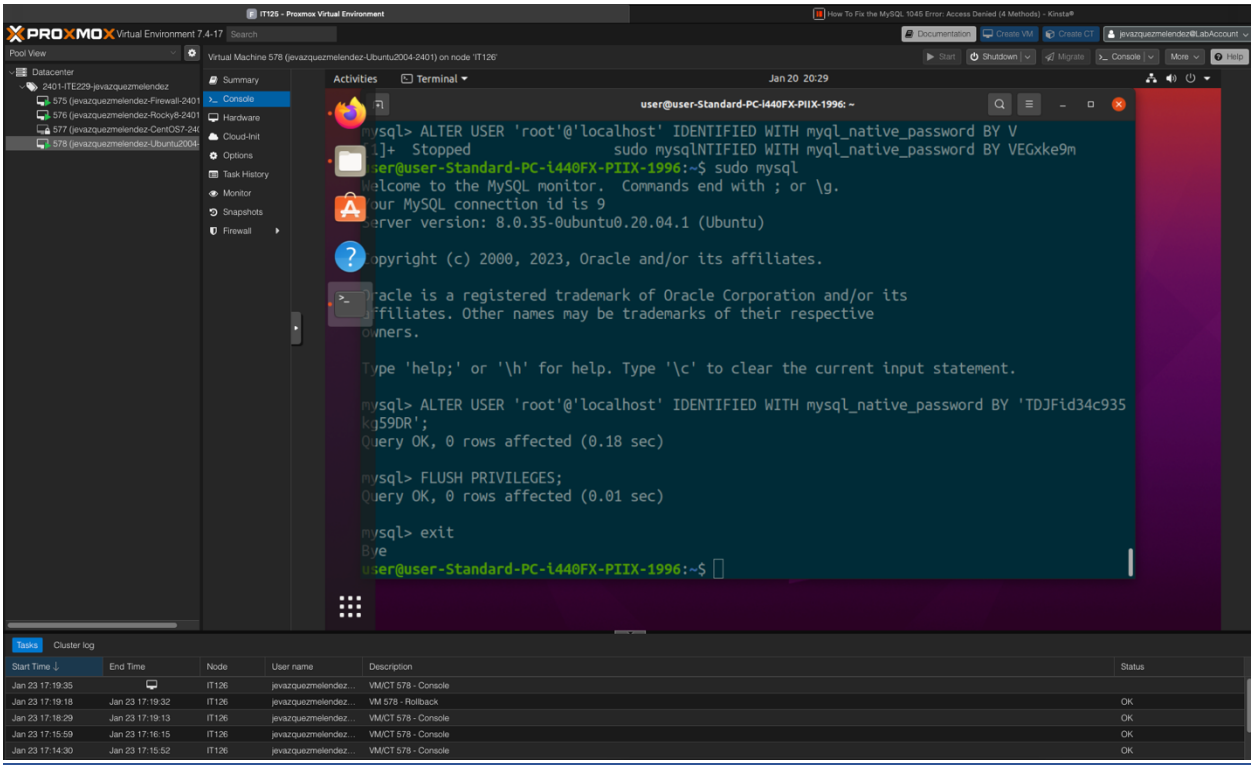
The command FLUSH PRIVILEGES; is used in MySQL to reload the grant tables and refresh the user privileges. This is useful when you have to make changes to the MySQL database user accounts or privileges and want to ensure that the changes take effect immediately.



Quit MySQL

mysql> exit

The exit command is used to quit the MySQL command-line interface. When you type this command and press Enter, the MySQL shell will close, and you will return to the ubuntu shell.



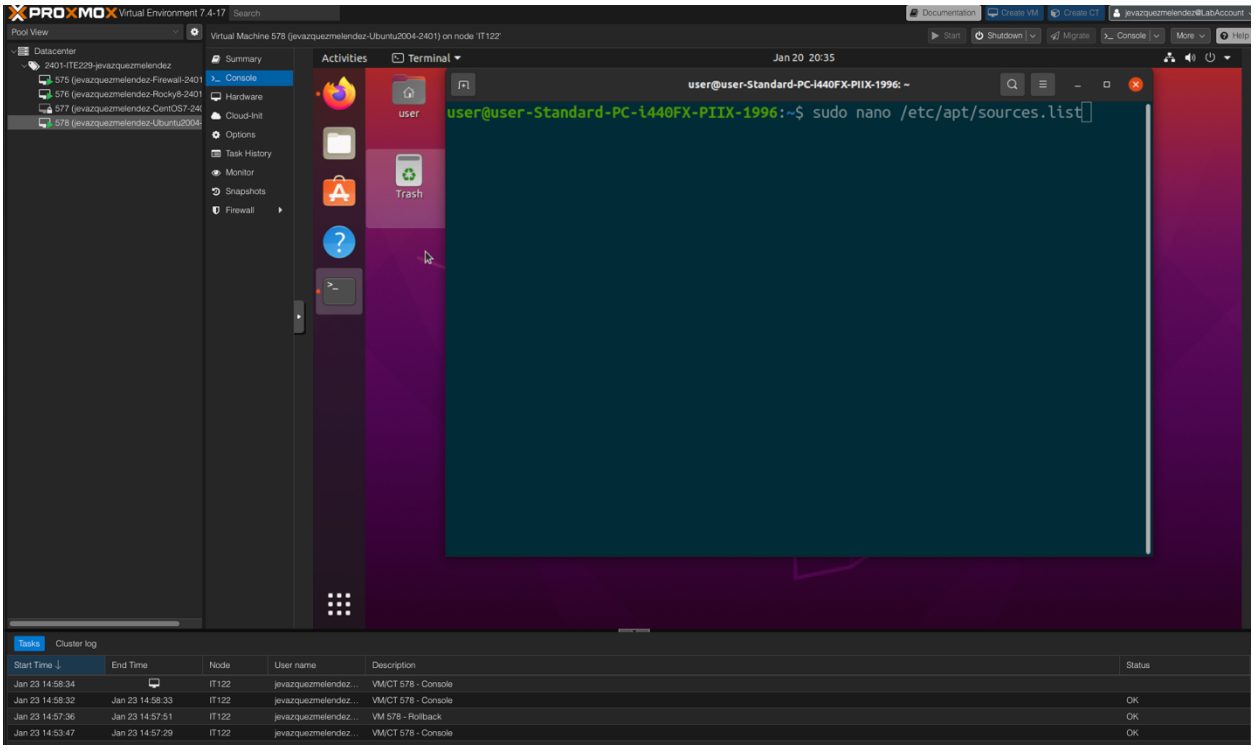
Install PHP

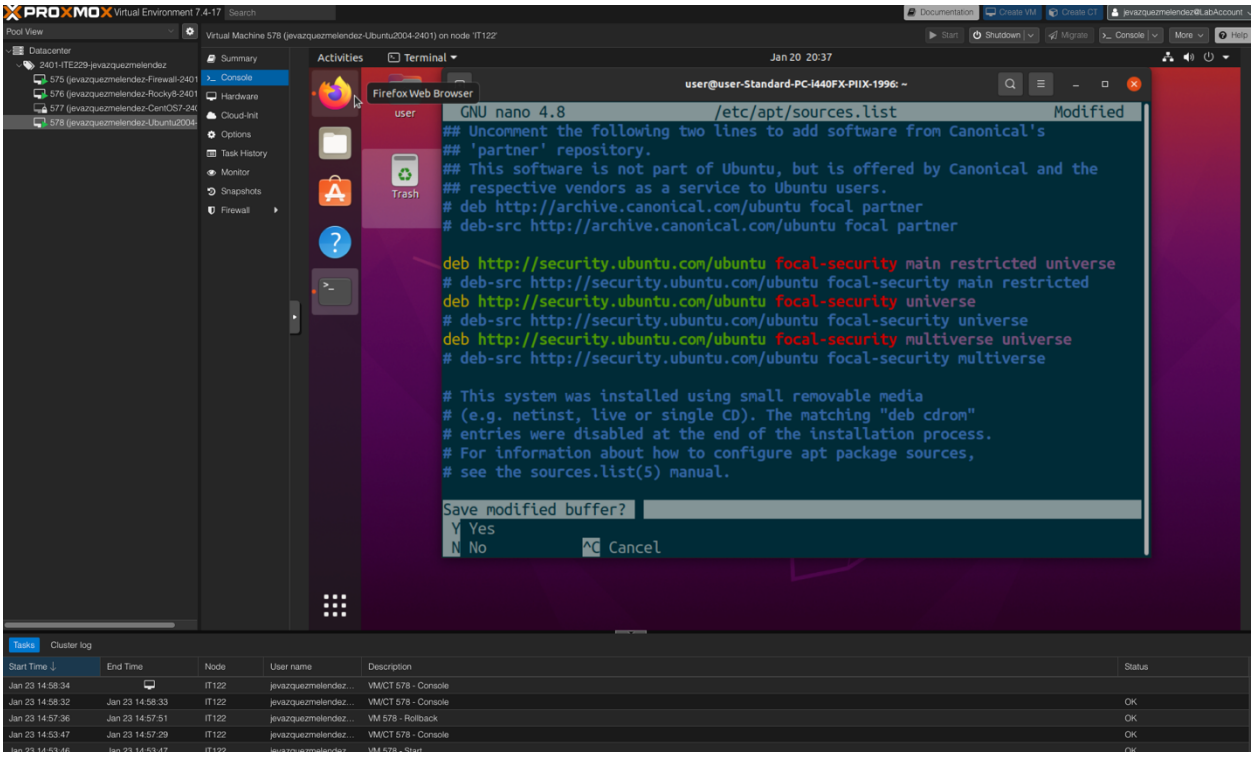
Edit Sources.list File

$ sudo nano /etc/apt/sources.list

To put it simply, you need to open the sources. The list file is located at /etc/apt/ using the nano text editor with sudo privileges.

Then, you need to add the "universe" repository to all the URLs listed in the file.



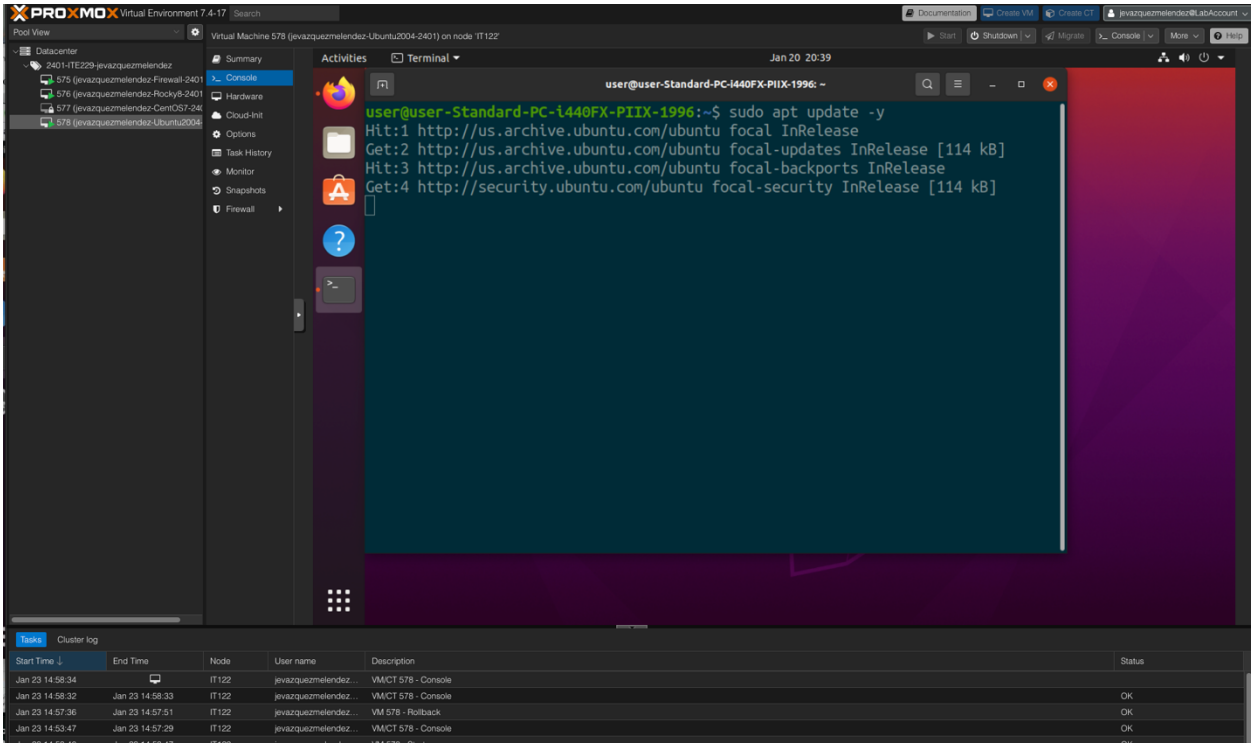

PROXMOX Virtual Environment 7.4-17
Search
Documentation
Create VM
Create CT
jevazquezmelendez@LabAccount
Pool View
Virtual Machine 578 (jevazquezmelendez-Ubuntu2004-2401) on node 'IT122'
Start
Shutdown
Migrate
Console
More
Help
Datacenter
2401-ITE229-jevazquezmelendez
575 (jevazquezmelendez-Firewall-2401
576 (jevazquezmelendez-Rocky8-2401
577 (jevazquezmelendez-CentOS7-240
578 (jevazquezmelendez-Ubuntu2004-
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Snapshots
Firewall
Activities
Terminal
Jan 20 20:37
Firefox Web Browser
user
Trash
user@user-Standard-PC-I440FX-PIIX-1996: ~
GNU nano 4.8 /etc/apt/sources.list Modified
Uncomment the following two lines to add software from Canonical's
'partner' repository.
This software is not part of Ubuntu, but is offered by Canonical and the
respective vendors as a service to Ubuntu users.
deb http://archive.canonical.com/ubuntu focal partner
deb-src http://archive.canonical.com/ubuntu focal partner
deb http://security.ubuntu.com/ubuntu focal-security main restricted universe
deb-src http://security.ubuntu.com/ubuntu focal-security main restricted
deb http://security.ubuntu.com/ubuntu focal-security universe
deb-src http://security.ubuntu.com/ubuntu focal-security universe
deb http://security.ubuntu.com/ubuntu focal-security multiverse universe
deb-src http://security.ubuntu.com/ubuntu focal-security multiverse
This system was installed using small removable media
(e.g. netinst, live or single CD). The matching "deb cdrom"
entries were disabled at the end of the installation process.
For information about how to configure apt package sources,
see the sources.list(5) manual.
Save modified buffer?
Y Yes
N No
^C Cancel
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Jan 23 14:58:34 IT122 jevazquezmelendez... VM/CT 578 - Console
Jan 23 14:58:32 Jan 23 14:58:33 IT122 jevazquezmelendez... VM/CT 578 - Console OK
Jan 23 14:57:36 Jan 23 14:57:51 IT122 jevazquezmelendez... VM 578 - Rollback OK
Jan 23 14:53:47 Jan 23 14:57:29 IT122 jevazquezmelendez... VM/CT 578 - Console OK

Update Ubuntu (refreshes the repolist)

$ sudo apt update -y

After saving the changes, you need to update the repository list by running the sudo apt update -y.

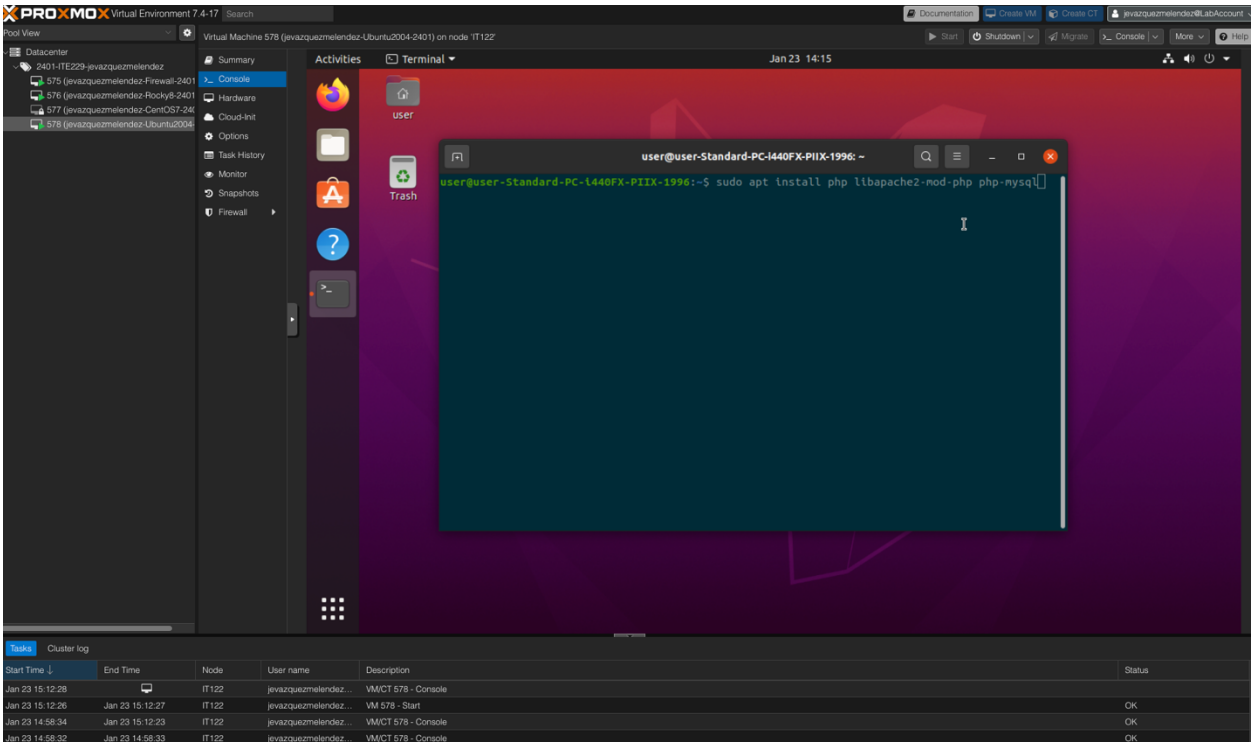
This command is needed so that the system can fetch the latest package information from the added repository.



Install Required PHP Libraries

$ sudo apt install php libapache2-mod-php php-mysql

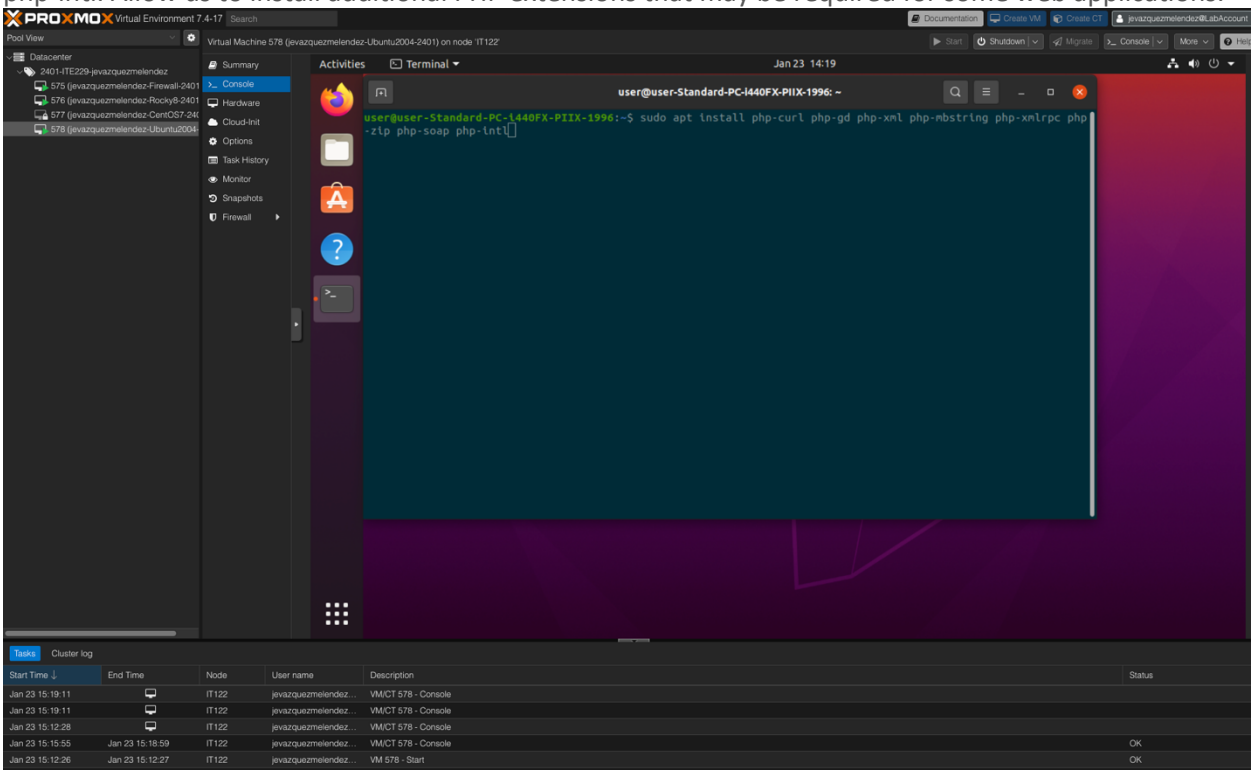
This command sudo apt install php libapache2-mod-php php-mysql. Is used to install PHP and its MySQL driver, as well as the Apache PHP module.



Install Required MySQL Libraries

$ sudo apt install php-curl php-curl php-gd php-xml php-mbstring php-xmlrpc php-zip php-soap php-intl

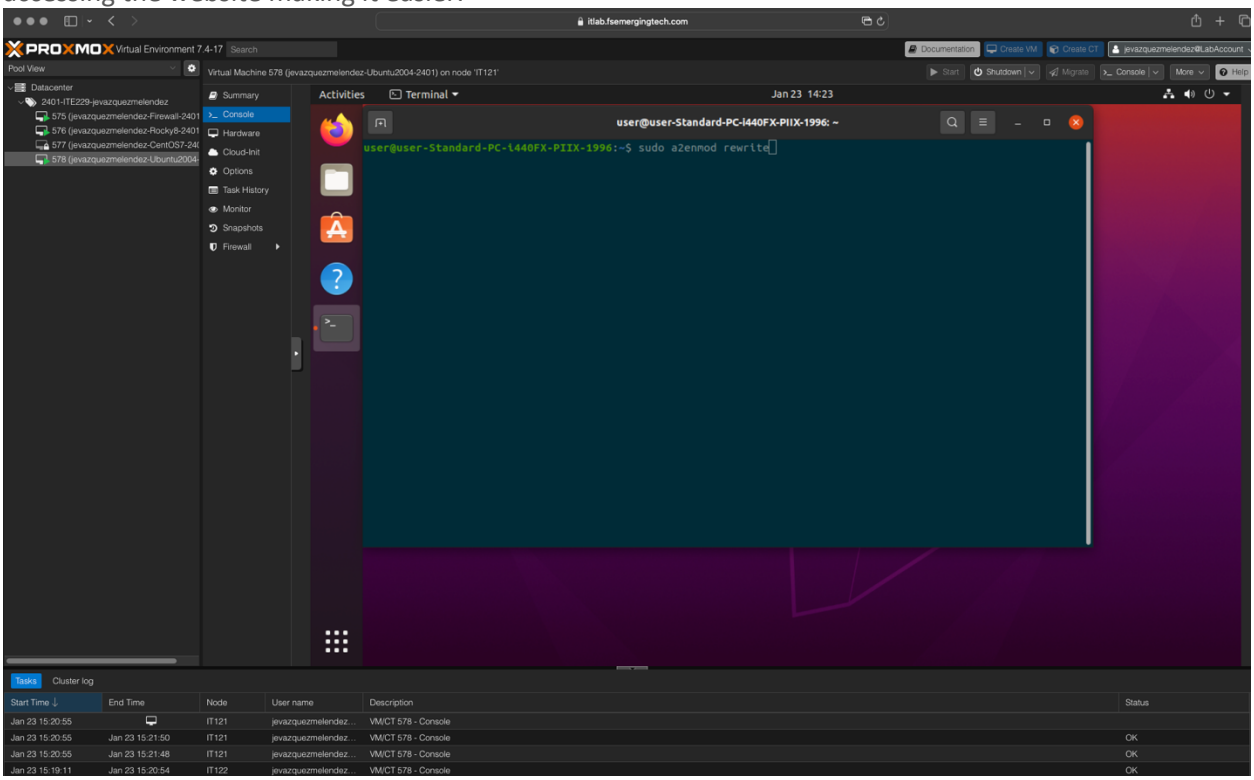
This command sudo apt install php-curl php-curl php-gd php-xml php-mbstring php-xmlrpc php-zip php-soap php-intl. Allow us to install additional PHP extensions that may be required for some web applications.



Enable URL Rewrites (clean URLs)

$ sudo a2enmod rewrite

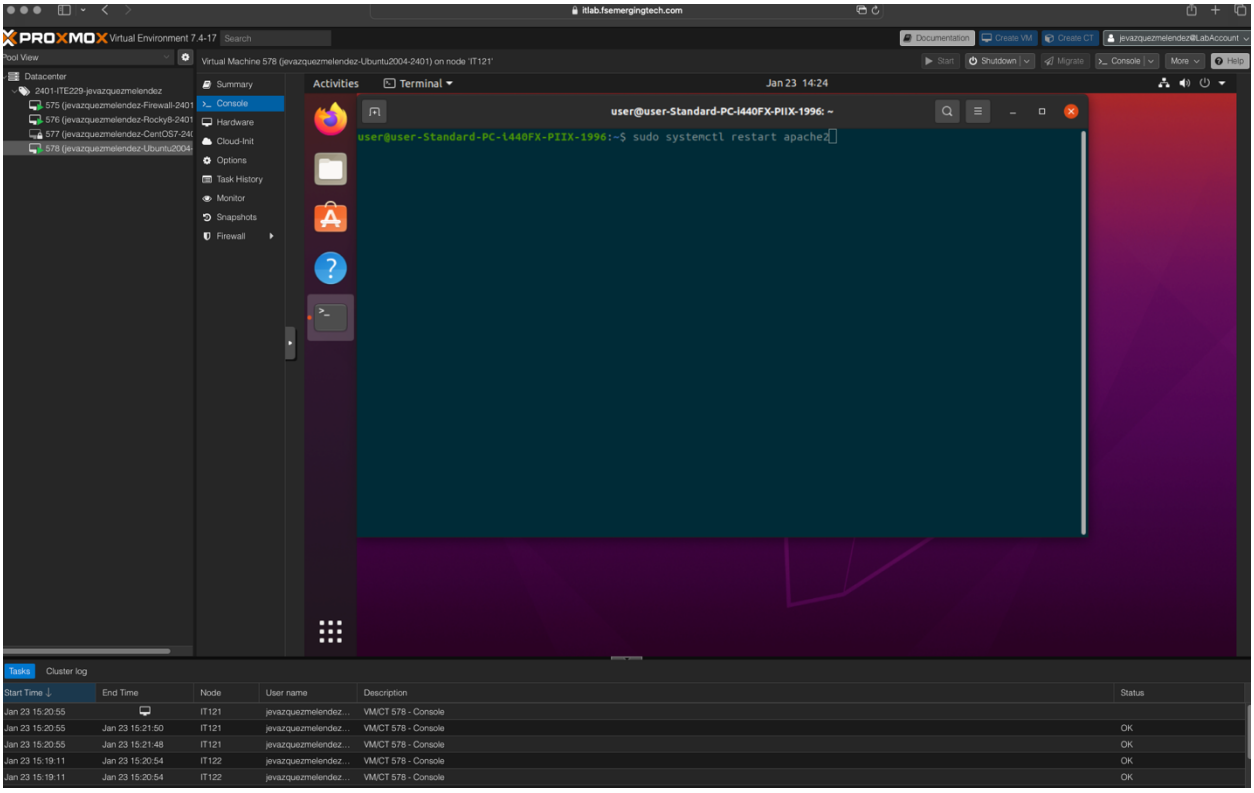
The command sudo a2enmod rewrite. Allow us to enable the Apache module mod_rewrite, which allows for URL rewriting and is commonly used in web applications to create clean URLs. This will benefit the user accessing the website making it easier.



Restart Apache Service

$ sudo systemctl restart apache2

This command, sudo systemctl restart apache2. Is used to restart the Apache web server software. This command is usually executed when there are some changes made to the configuration files of the web server.



Create a test.php Web Page

$ sudo nano /var/www/html/test.php

<?php phpinfo(); ?>

Press x and then y to save the file and exit nano.

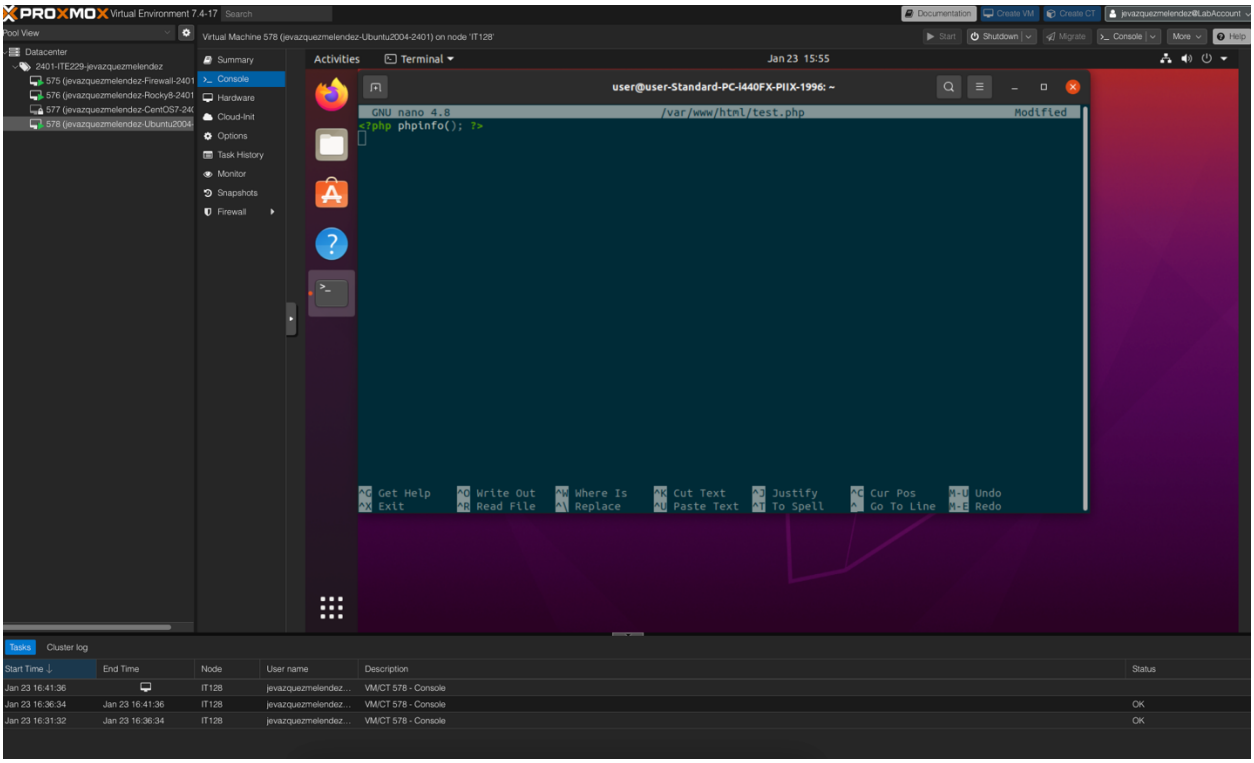
The command sudo nano /var/www/html/test.php, is used to open the test.php file in the nano text editor.

This file is located in the /var/www/html/ directory and contains a simple PHP script that displays the PHP configuration information.

After opening the file in Nano, you need to add the code:

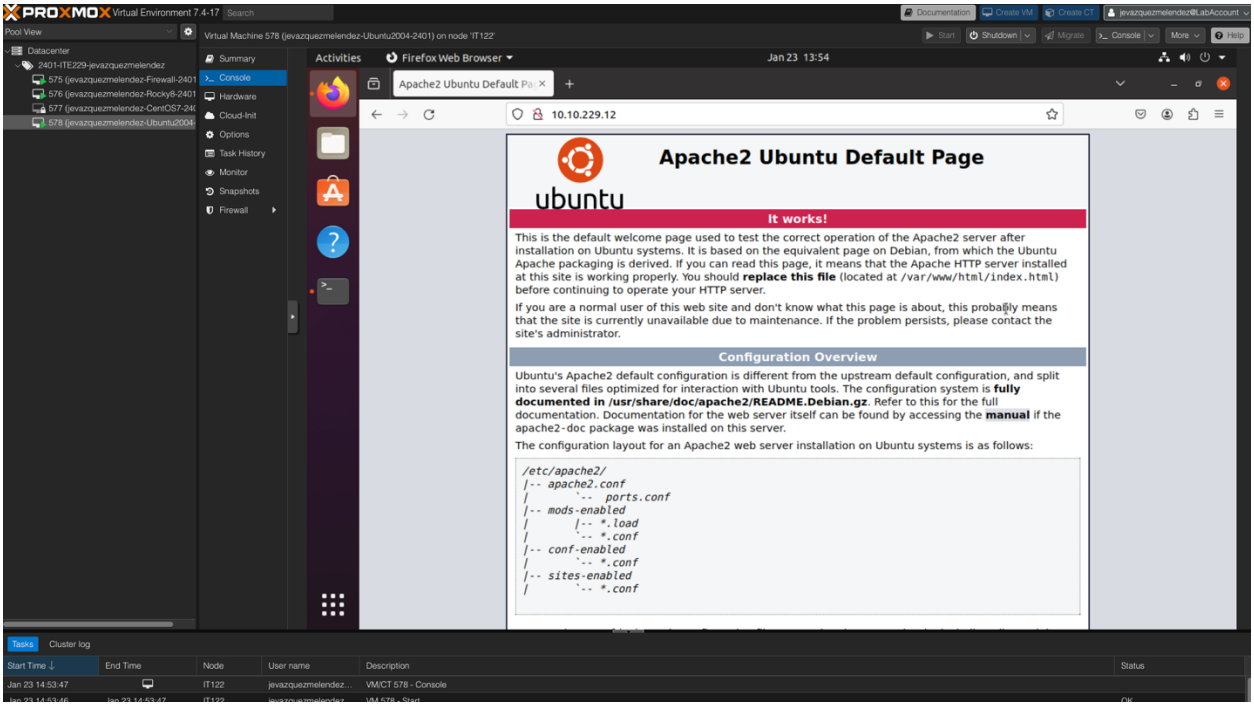
<?php phpinfo(); ?>

This code will display the PHP configuration information on the web page. To save the changes made to the file, you need to press 'x' to exit the editor and then 'y' to save the changes.



Test the test.php Web Page

Open the Firefox Web Browser. Once you have saved the changes, you can test the web page of the test.php using the IP address 10.10.229.12/test.php to connect to the server where the Apache web is running.

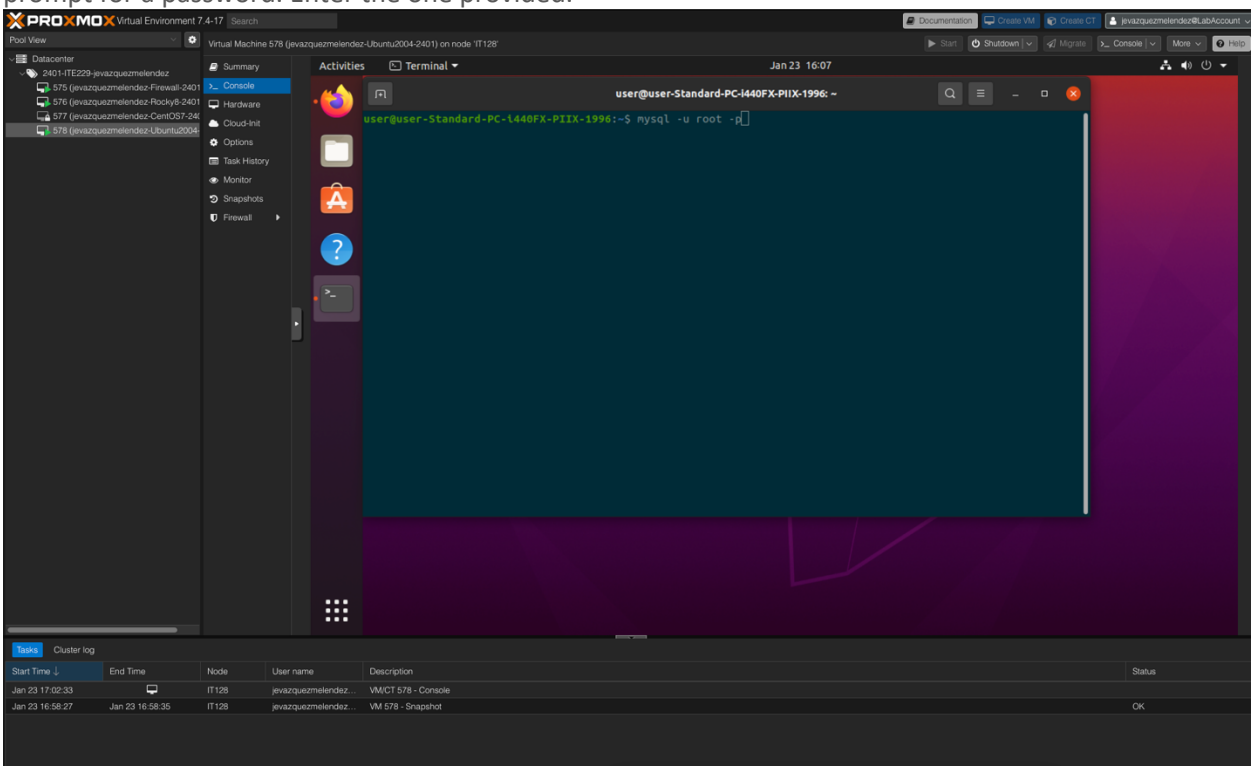


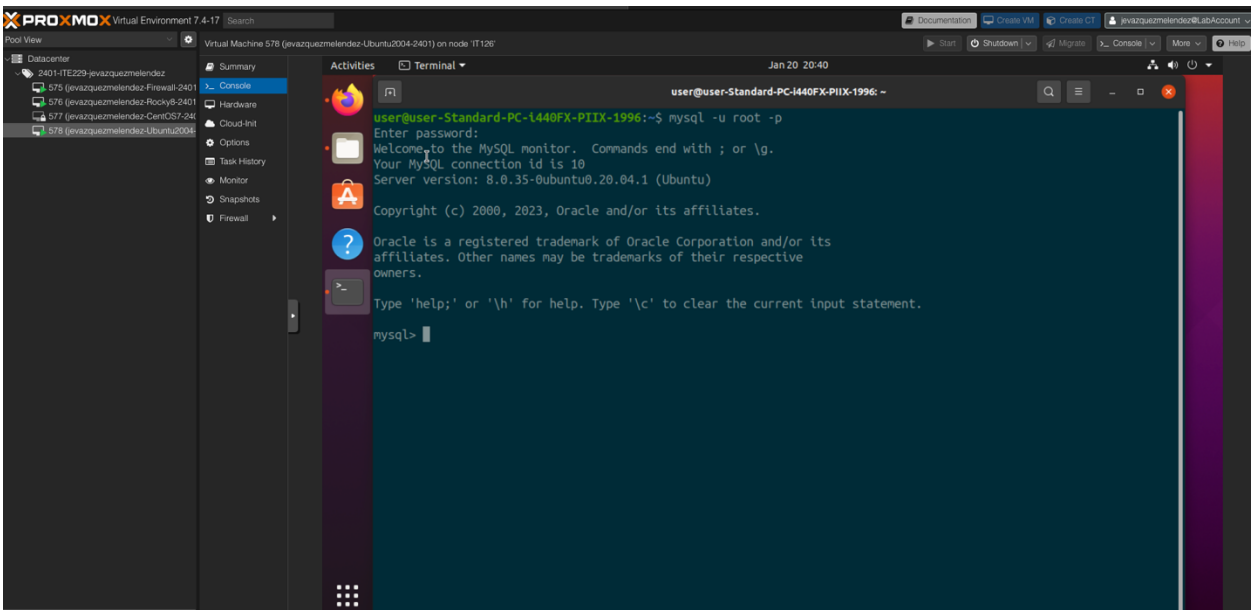
Database Configuration in MySQL

Log into MySQL Database

$ mysql -u root -p

The command "mysql -u root -p" is used to log in to the MySQL database with the user "root" and it will prompt for a password. Enter the one provided.

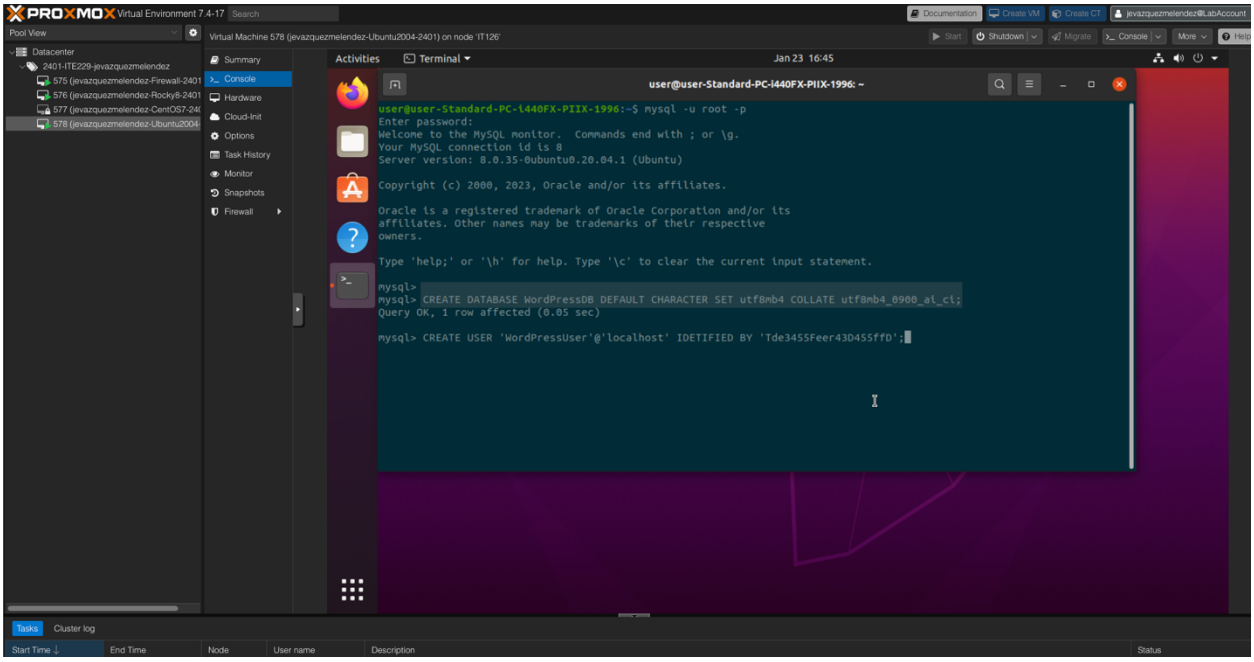




Create WordPress Database in MySQL

mysql> CREATE DATABASE WordPressDB DEFAULT SET utf8mb4 COLLATE uft8mb4_0900_ai_ci;

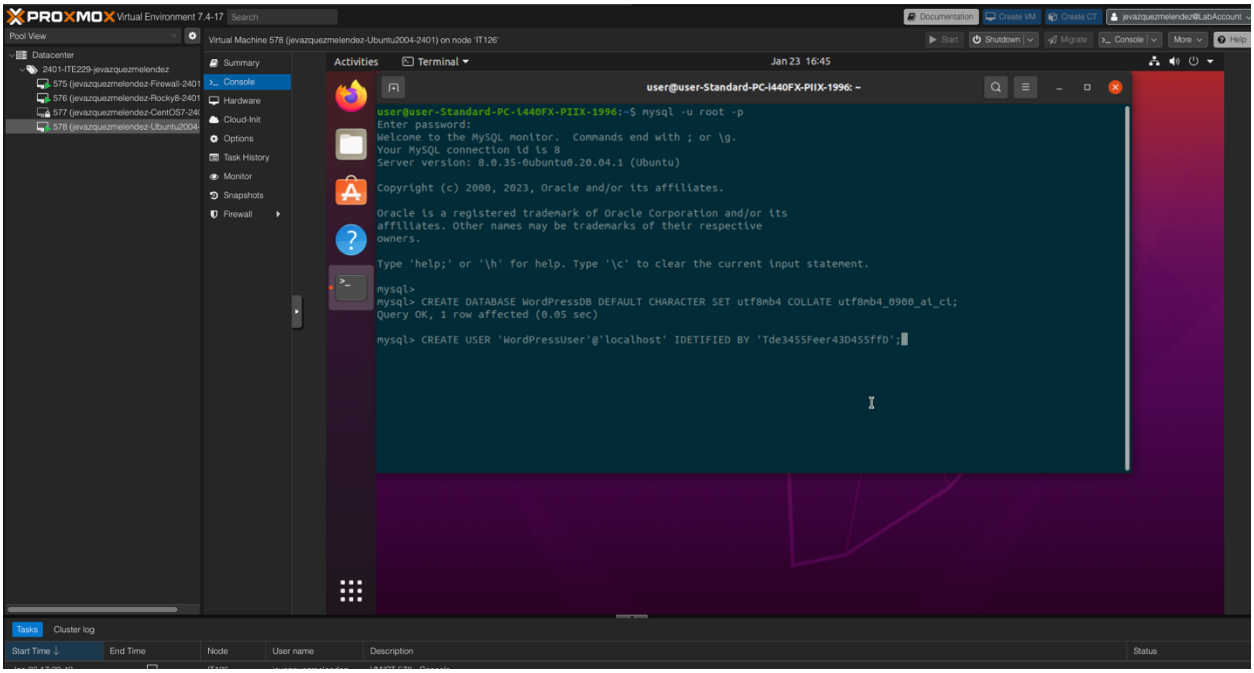
The command CREATE DATABASE WordPressDB DEFAULT SET utf8mb4 COLLATE uft8mb4_0900_ai_ci. Is used to create a new database named "WordPressDB" with a default character set of "utf8mb4" and a specific collation of uft8mb4_0900_ai_ci.



Create WordPress User for MySQL Database

Mysql> CREATE USER ‘WordPressUser’@’localhost’ IDENTIFIED BY ‘Tde3455Fr43D455ffD’;

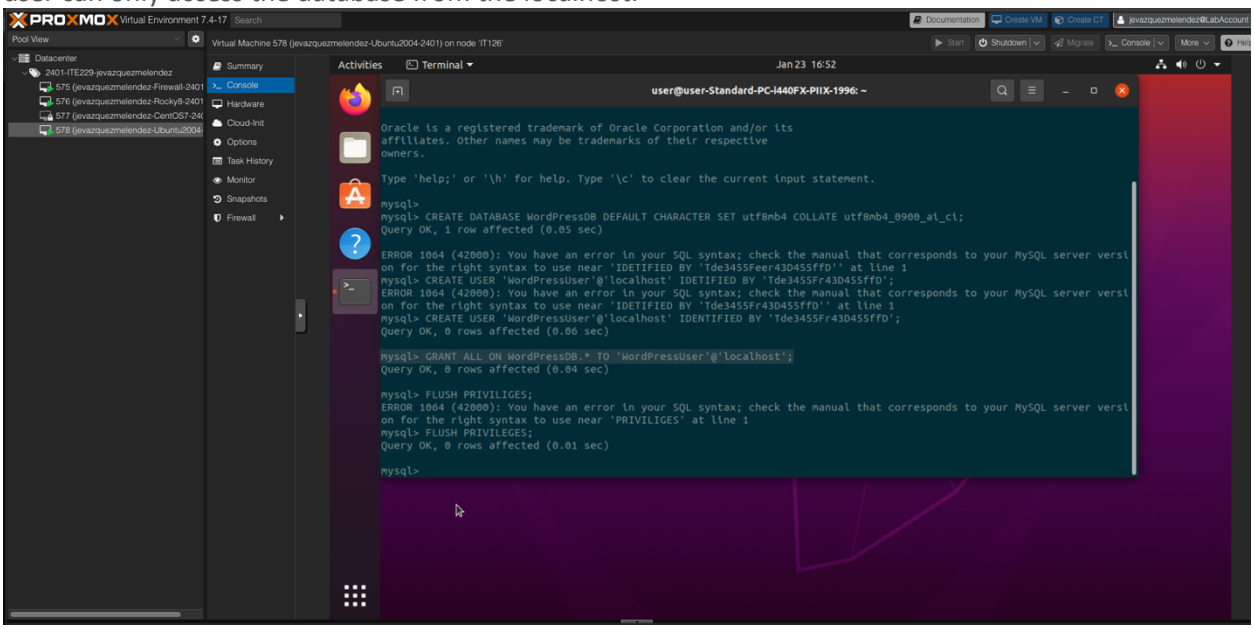
This is used to create a new user in the MySQL database system named "WordPressUser". The keyword " IDENTIFIED BY ‘Tde3455Fr43D455ffD’; ” is used to set as a password for the user.



Grant Privileges to this New WordPress User

Mysql> GRANT ALL ON WordPressDB.* TO ‘WordPressUser’@’localhost’;

The command mysql> GRANT ALL ON WordPressDB.* TO ‘WordPressUser’@’localhost’, is used to grant all privileges to a user named "WordPressUser" on the newly created "WordPressDB" database, and this user can only access the database from the localhost.

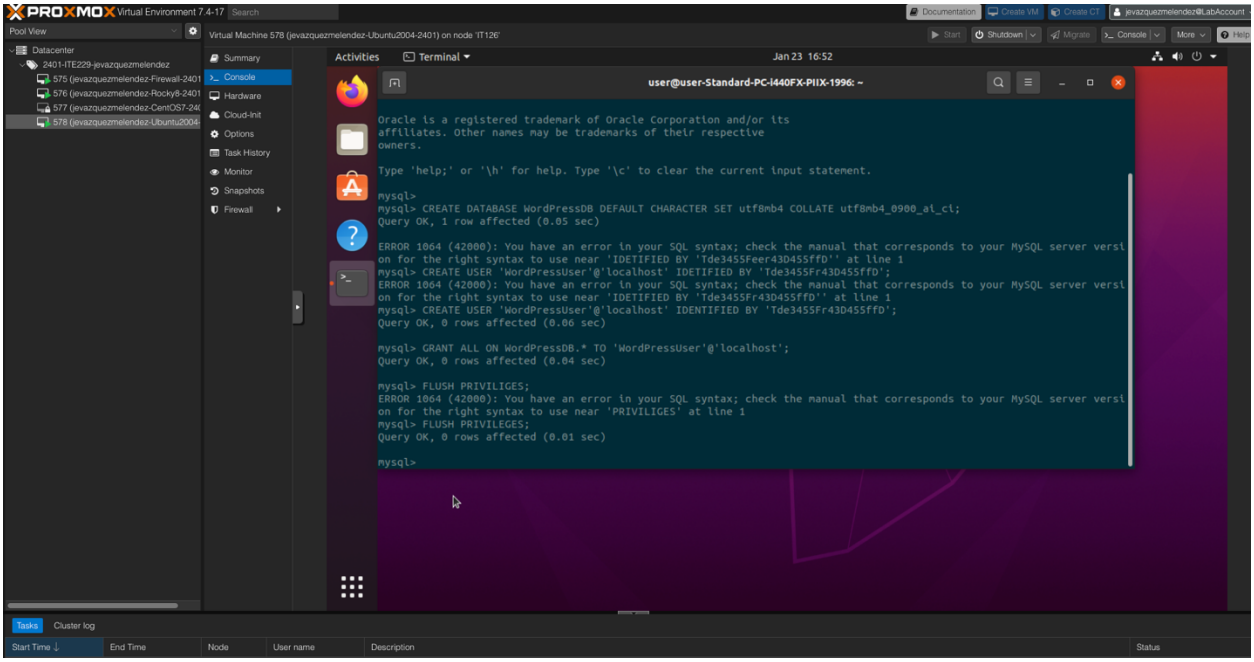


Flush Privileges

mysql> FLUSH PRIVILEGES;

The command mysql> FLUSH PRIVILEGES;

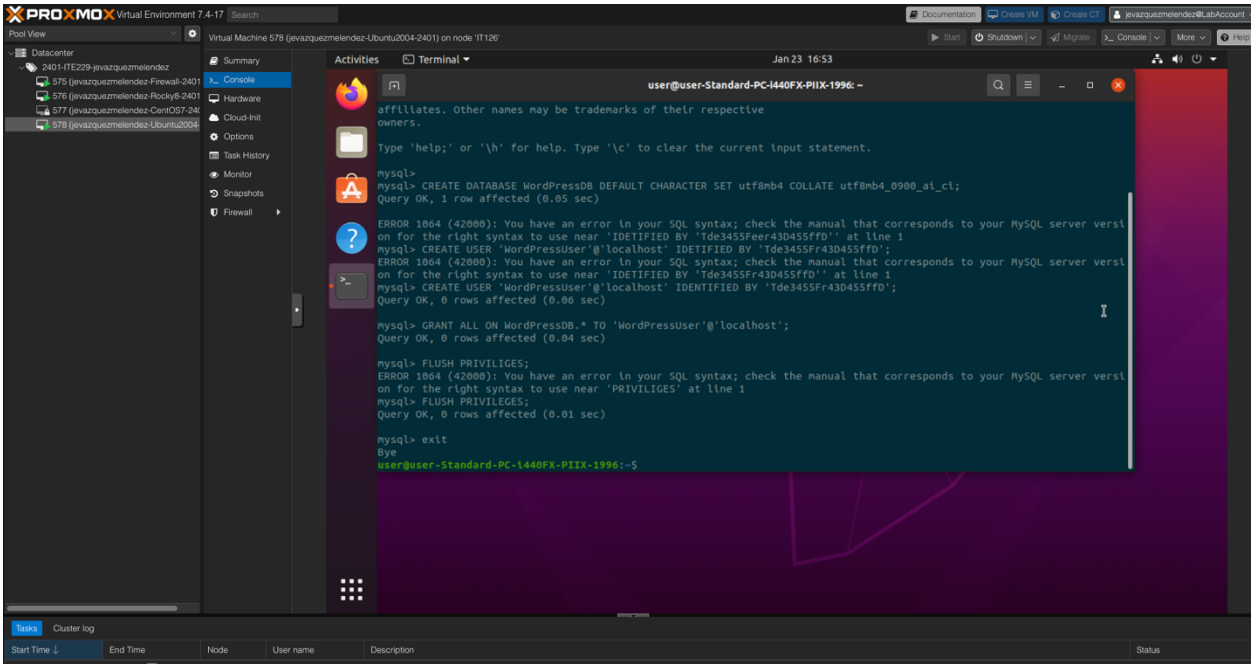
It is used to apply the changes made in the previous step and reload the privileges table in the database.



Quit MySQL

mysql> exit

The exit command is used to quit the MySQL command-line interface. When you type this command and press Enter, the MySQL shell will close, and you will return to the ubuntu shell.

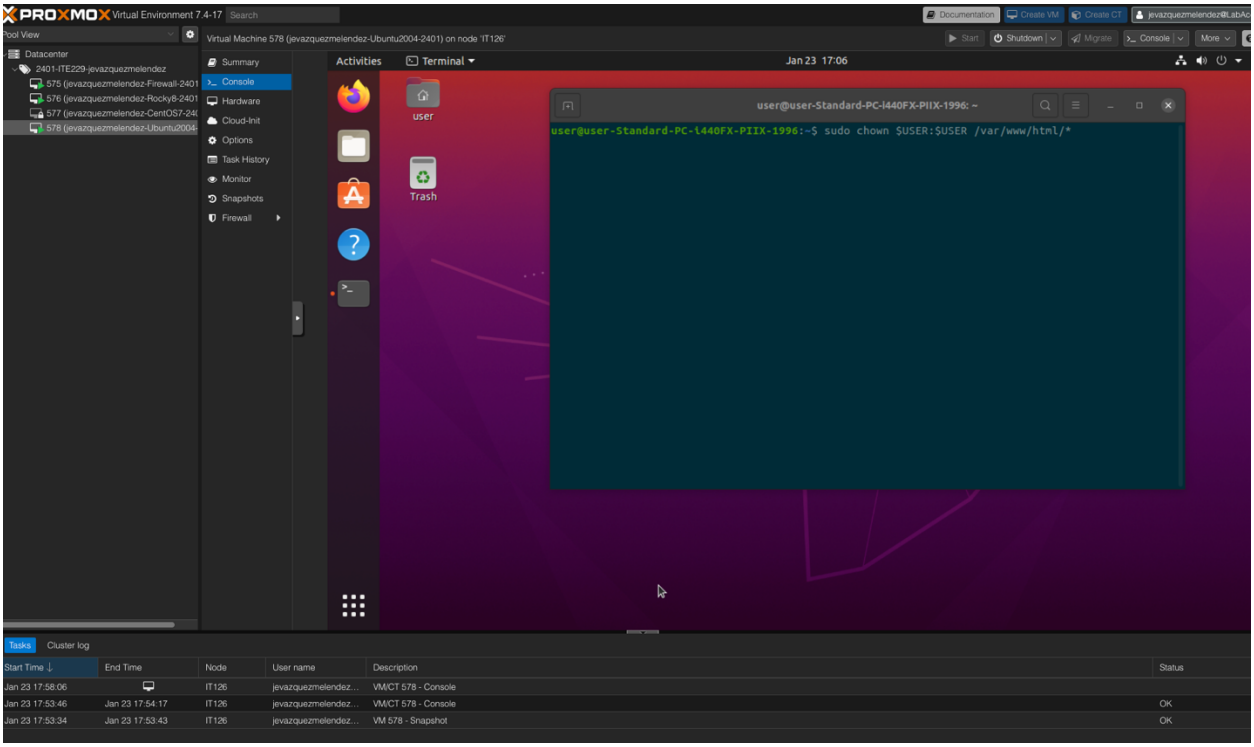


Install WordPress

Grant Permission to html Directory to WordPress User

$ sudo chown $USER:$USER /var/www/html/*

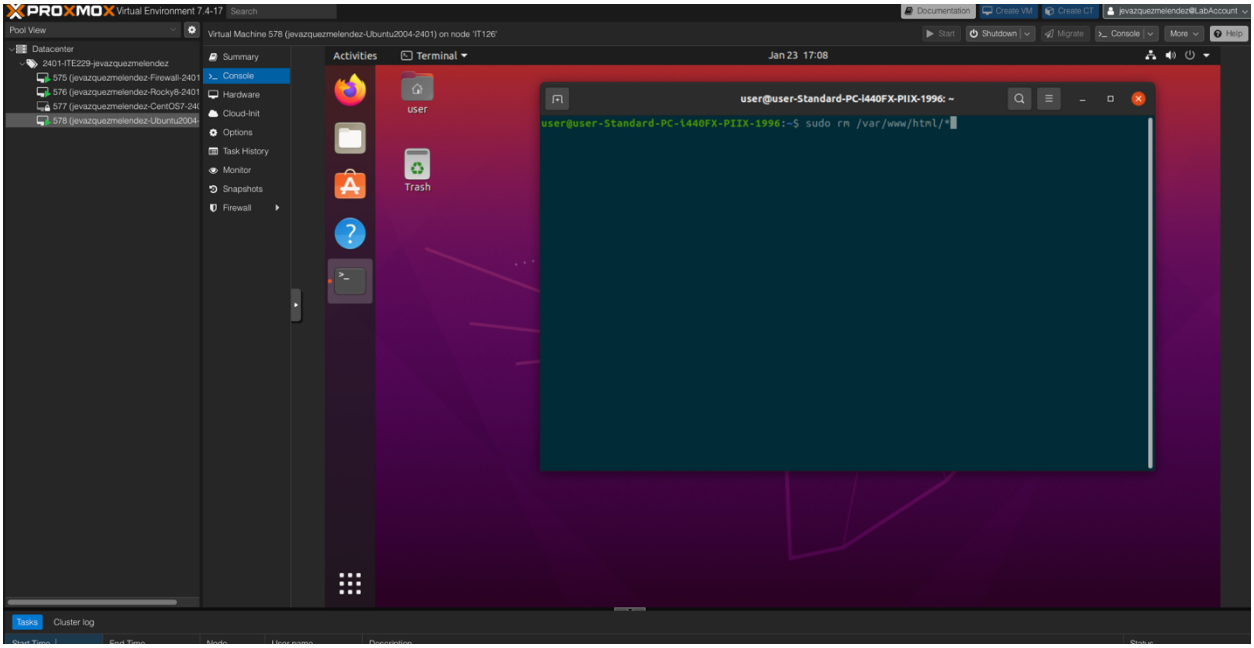
This command is going to allow us to change the ownership of all files and directories inside the /var/www/html folder to the current user.



Delete Files from html Directory

$ sudo rm /var/www/html/*

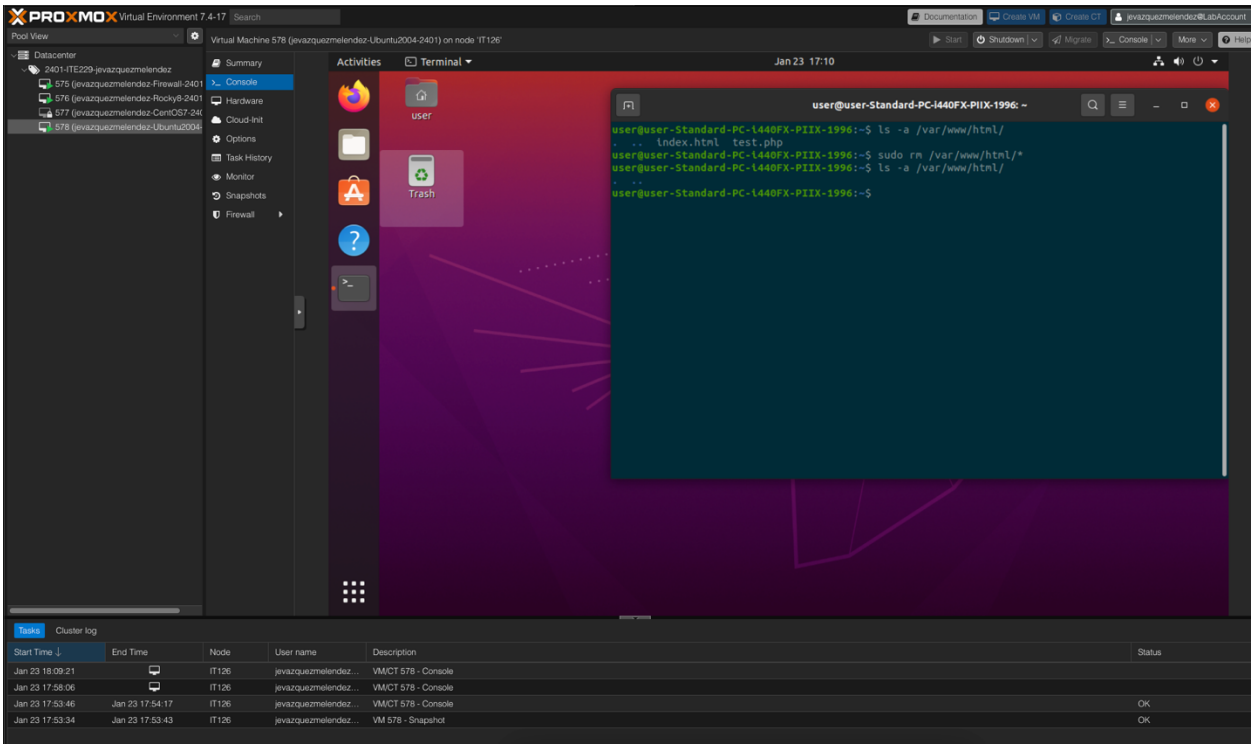
To Remove files in the html directory we are going to use sudo rm /var/www/html/*. This command will delete all files and directories inside the /var/www/html folder.



Verify html Directory is Empty

$ ls -a /var/www/html/

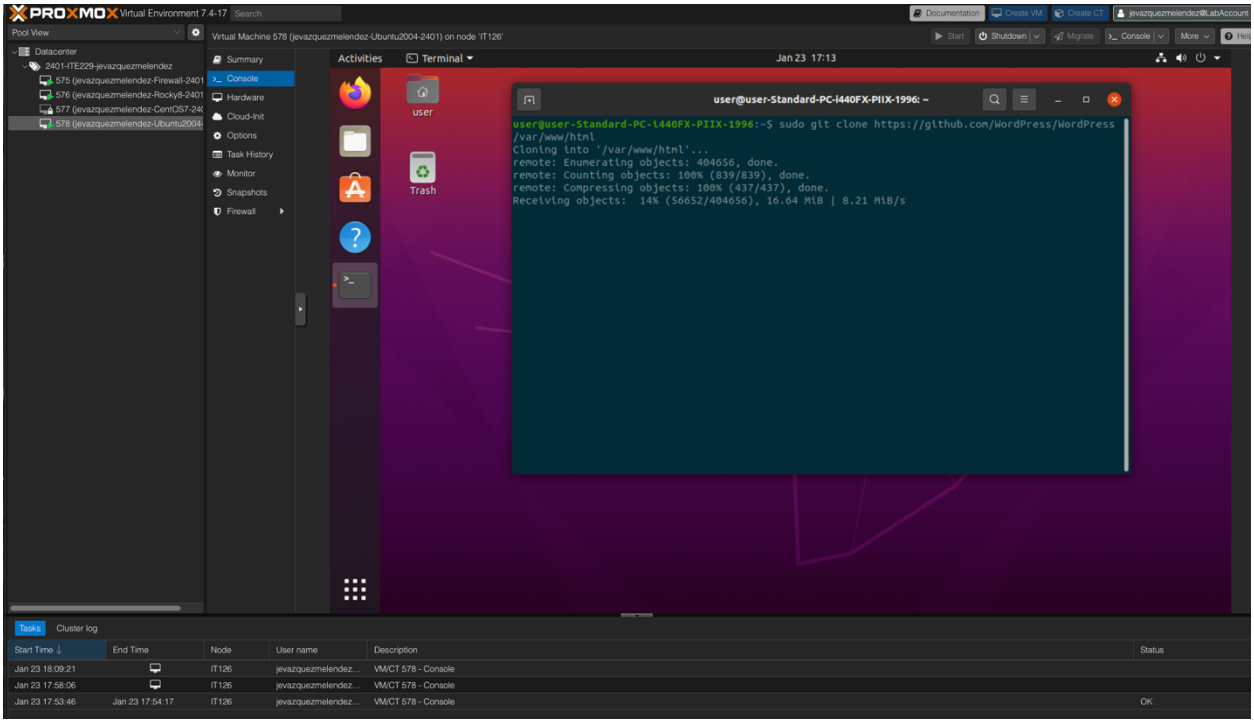
This command uses ls -a /var/www/html/ to lists all files and directories inside the /var/www/html folder, including the hidden ones.



Clone WordPress to html Directory

$ sudo git clone https://github.com/WordPress/WordPress/ /var/www/html

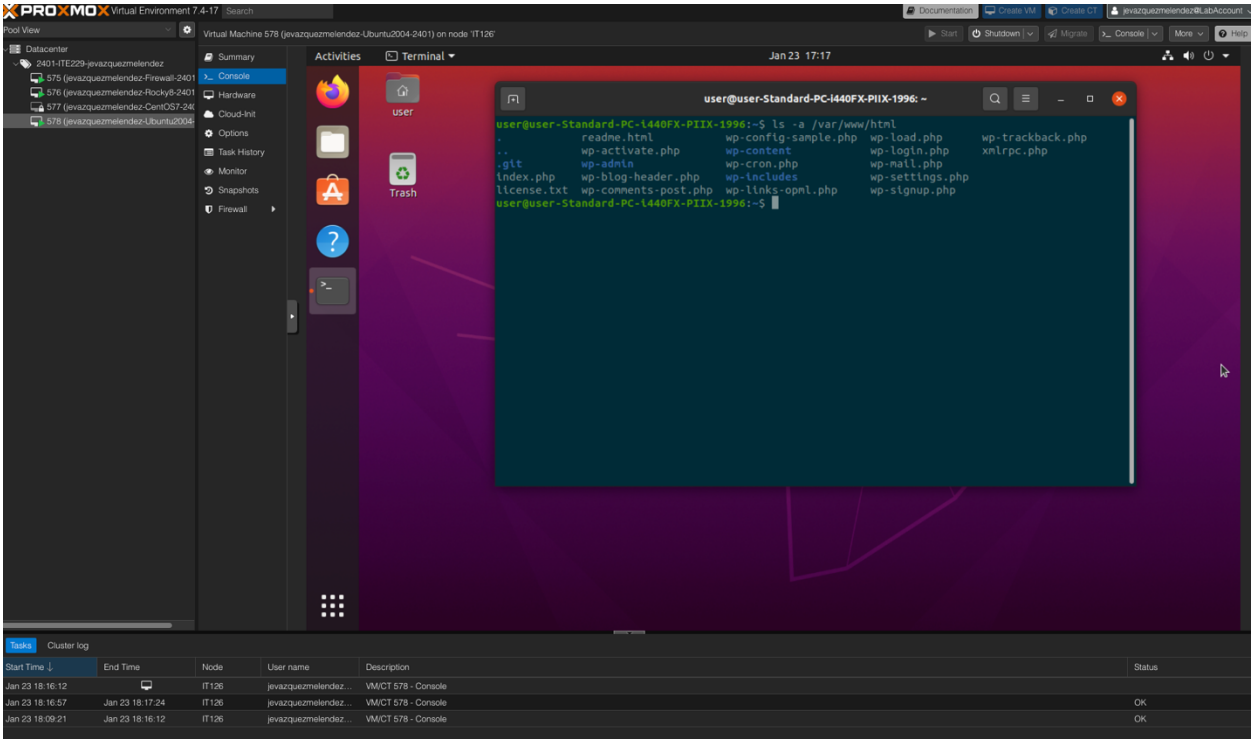
This is the command that we are going to use to clone a Git repository. We are cloning it from a specified URL and saves it in the /var/www/html folder.



Verify html Directory Contains WordPress Files

$ ls -a /var/www/html/

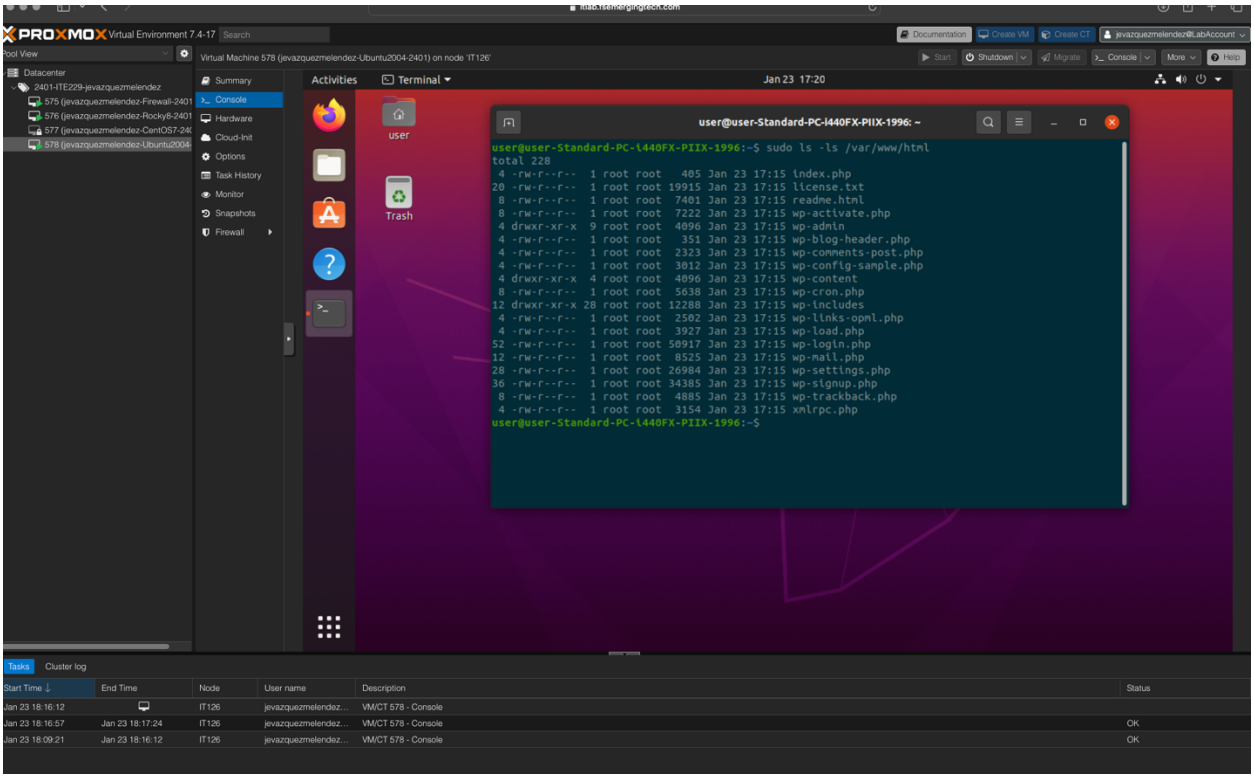
This command uses ls -a /var/www/html to lists all files and directories inside the /var/www/html folder, including the hidden ones.



Verify Permissions on html Directory

$ sudo ls -ls /var/www/html

Typing the following command sudo ls -ls /var/www/html. A list of all files and directories inside the /var/www/html folder with detailed information about their size and permissions.

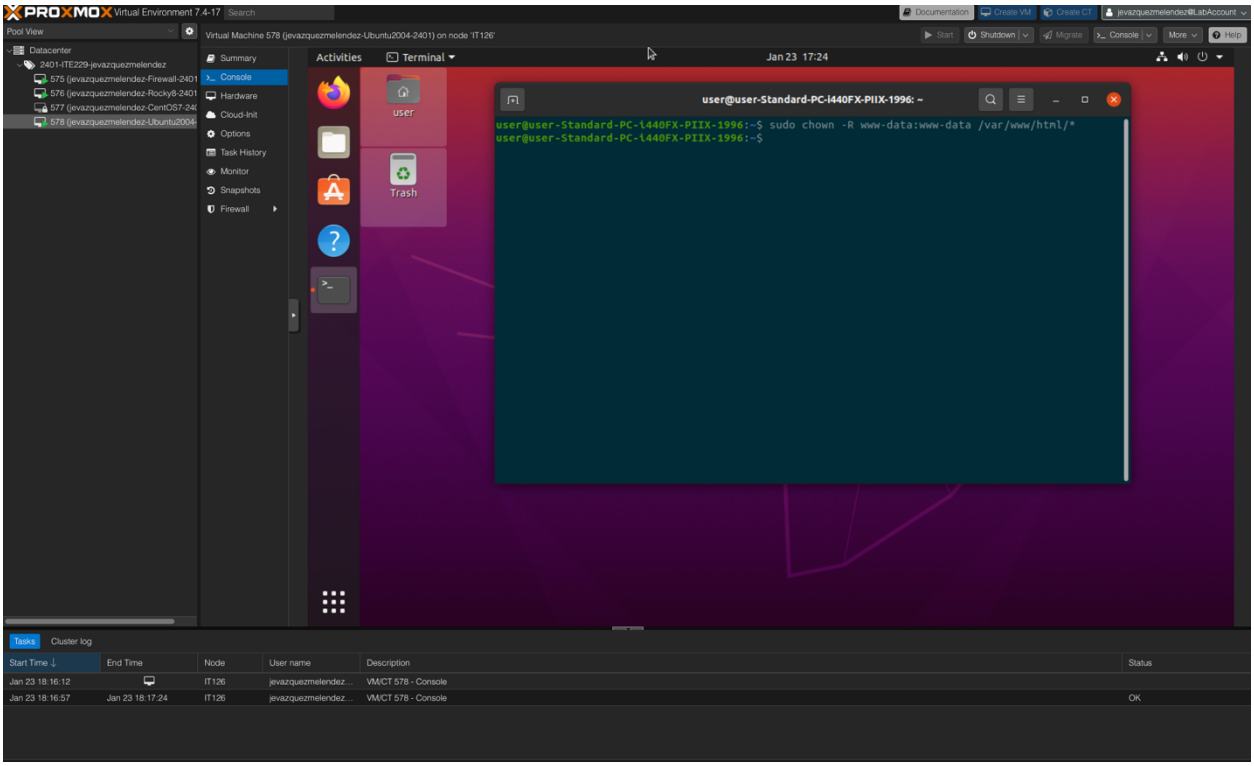


Edit Ownership

Edit Ownership of Contents of html Directory

$ sudo chown -R www-data:www-data /var/www/html/*

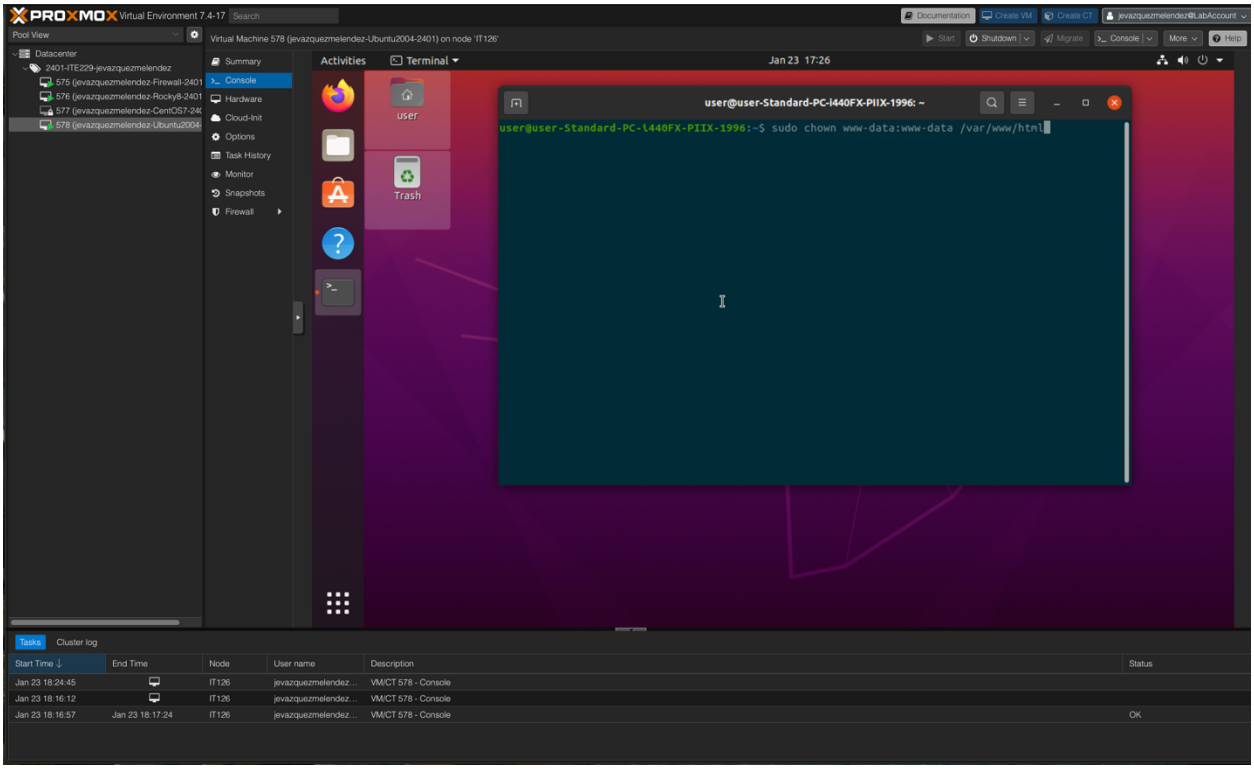
The following command using sudo privileges sudo chown -R www-data:www-data /var/www/html/ will make changes to the ownership of all files and directories inside the /var/www/html folder to the www-data user and group.



Edit Ownership of the html Directory Itself

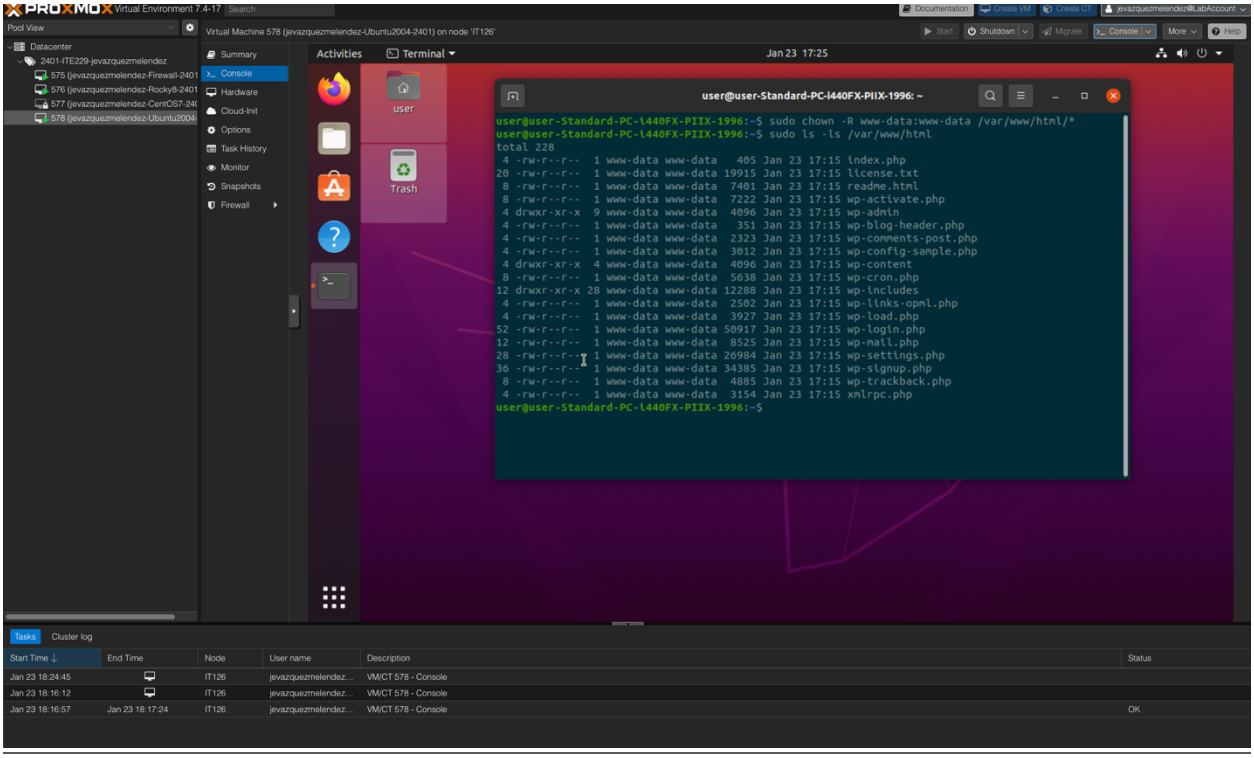
$ sudo chown www-data:www-data /var/www/html

To edit ownership of the html Directory we use the following command sudo chown www-data:www-data /var/www/html. This will make changes in the ownership of /var/www/html folder and assing in to the www-data user and group.



$ sudo ls -ls /var/www/html

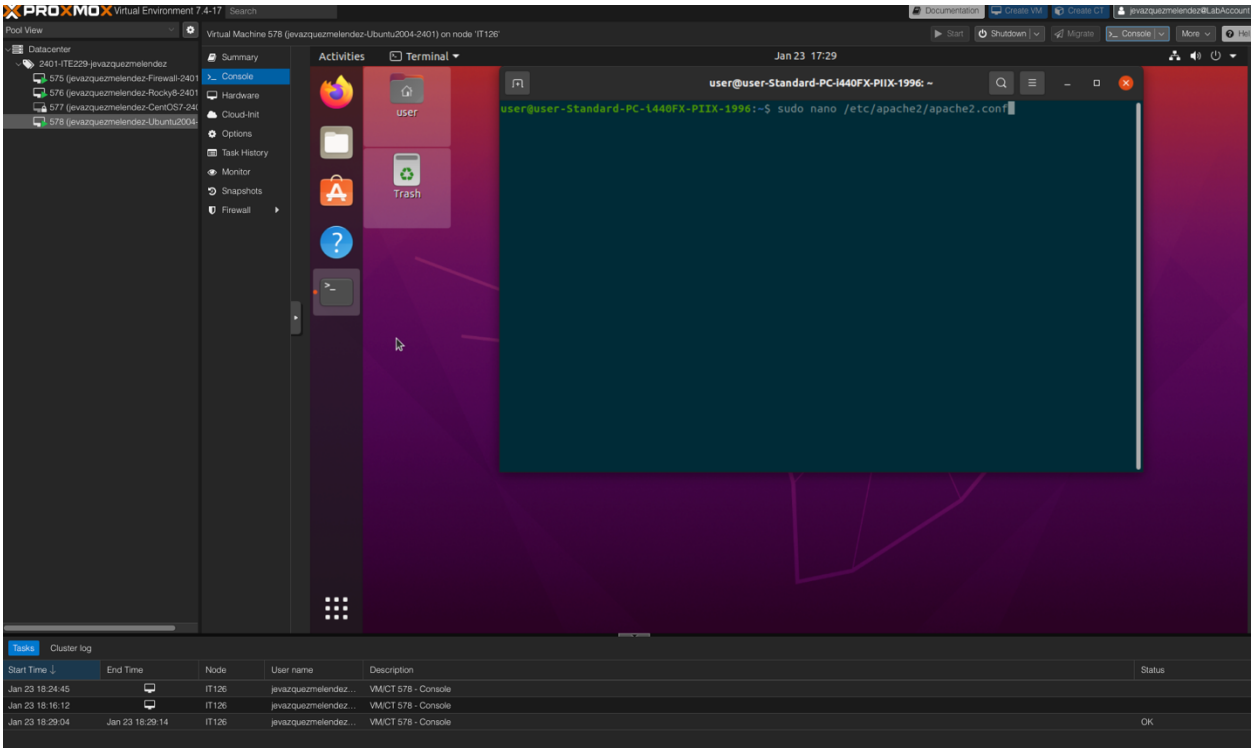
To verify the changes are made correctly.



Edit the apache2.conf File

$ sudo nano /etc/apache2/apache2.conf

Using this command to edit our apache2.conf file using nano our text editor. In this location is where the Apache configuration file is on your system. When you run this command, it will open the configuration file in the nano text editor, allowing you to make changes to the file as needed.

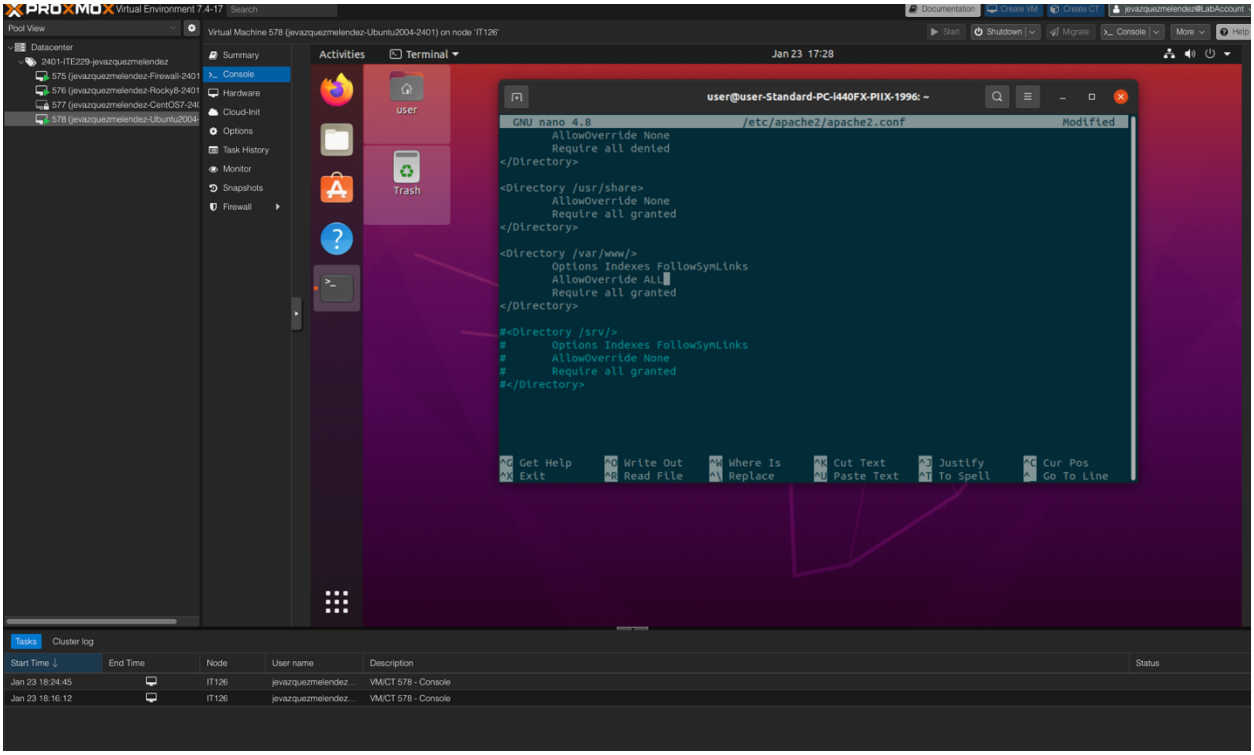


Override All Default Apache Directives

Here we are going to change the default setting to:

AllowOverride “ALL”

This will add an extra layer of security.

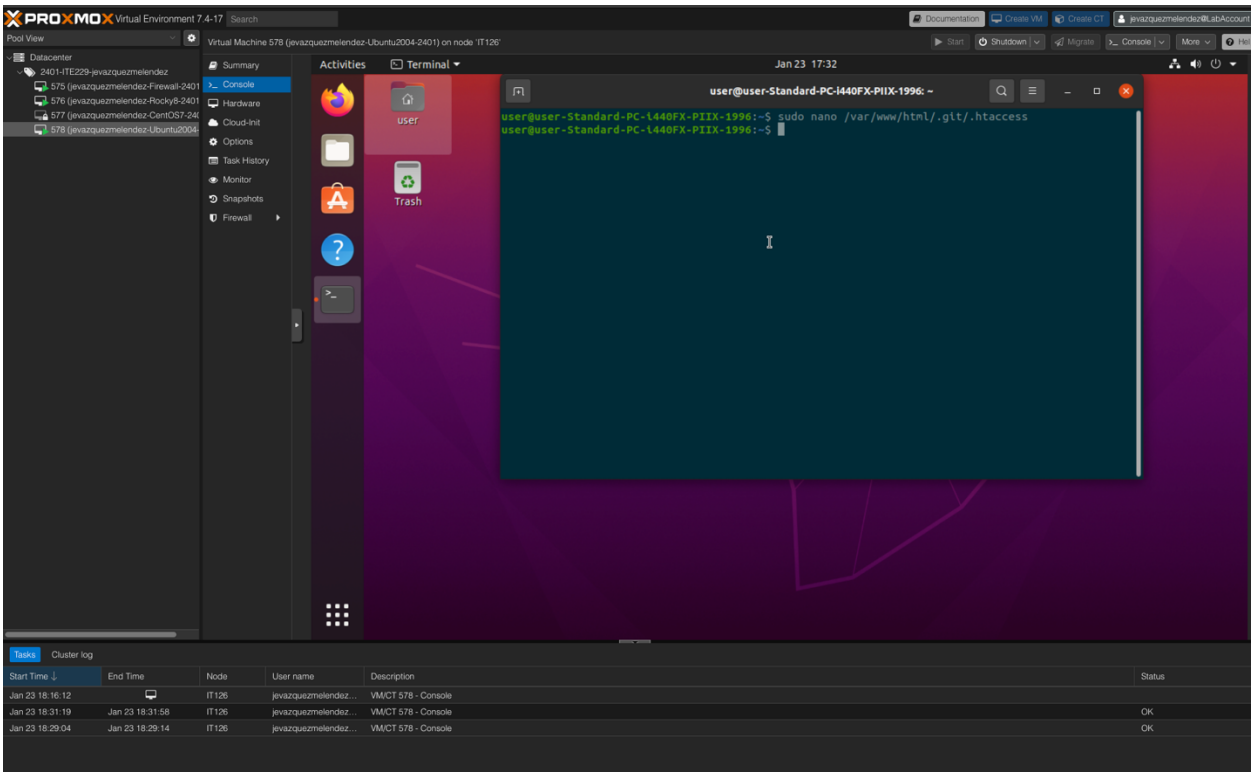


Create a .htaccess File in the /var/www/html/.git/ Directory

$ sudo nano /var/www/html/.git/.htacces

The command sudo nano /var/www/html/.git/.htaccess

This creates using the Nano text editor the file ".htaccess" located in the "/var/www/html/.git/" directory. This file is used to configure access restrictions for the Apache web server.

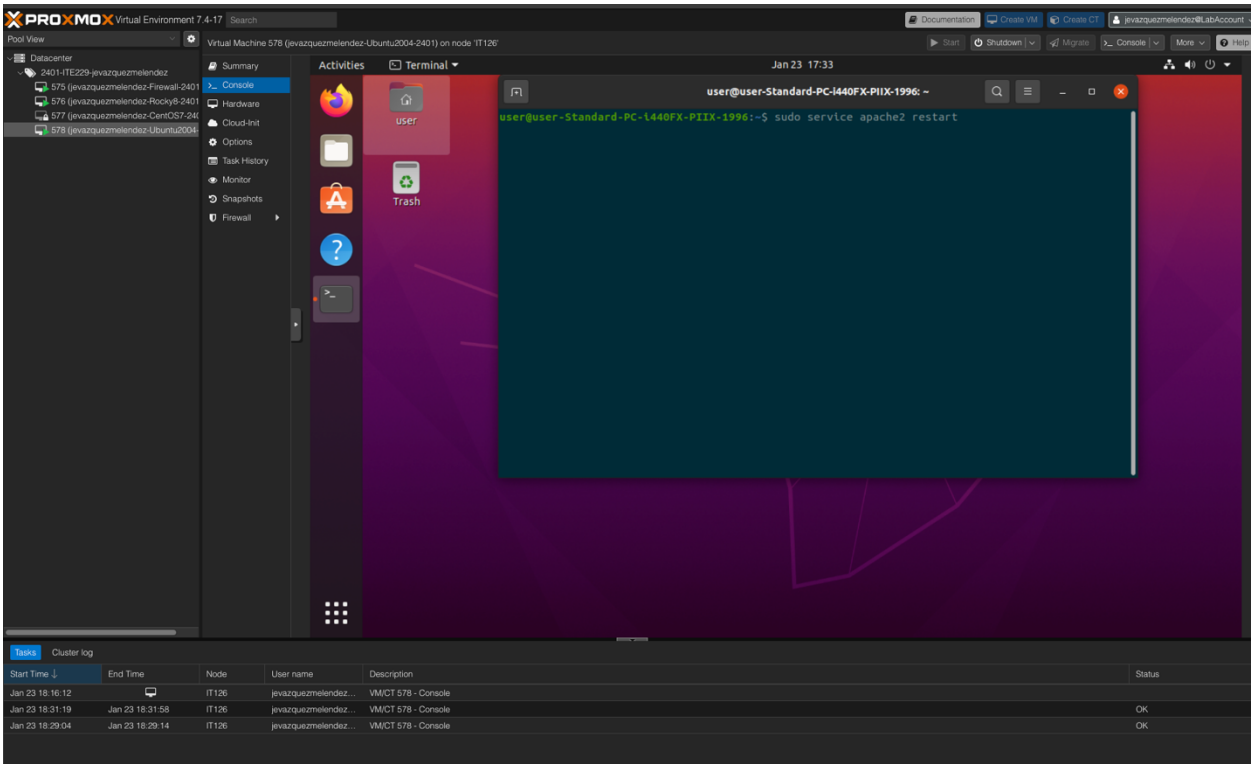


Restart the Apache Service

$ sudo service apache2 restart

Using this command sudo service apache2 restart. Restart the Apache web server.

This is necessary when changes are made to Apache's configuration files, such as the .htaccess file mentioned above, to ensure that the changes take effect.



IMPORTANT: To earn full credit, original formatting of this document must remain in place. In addition, ALL screenshots must include a “full view”, including your ProxMox title bar with your username showing.

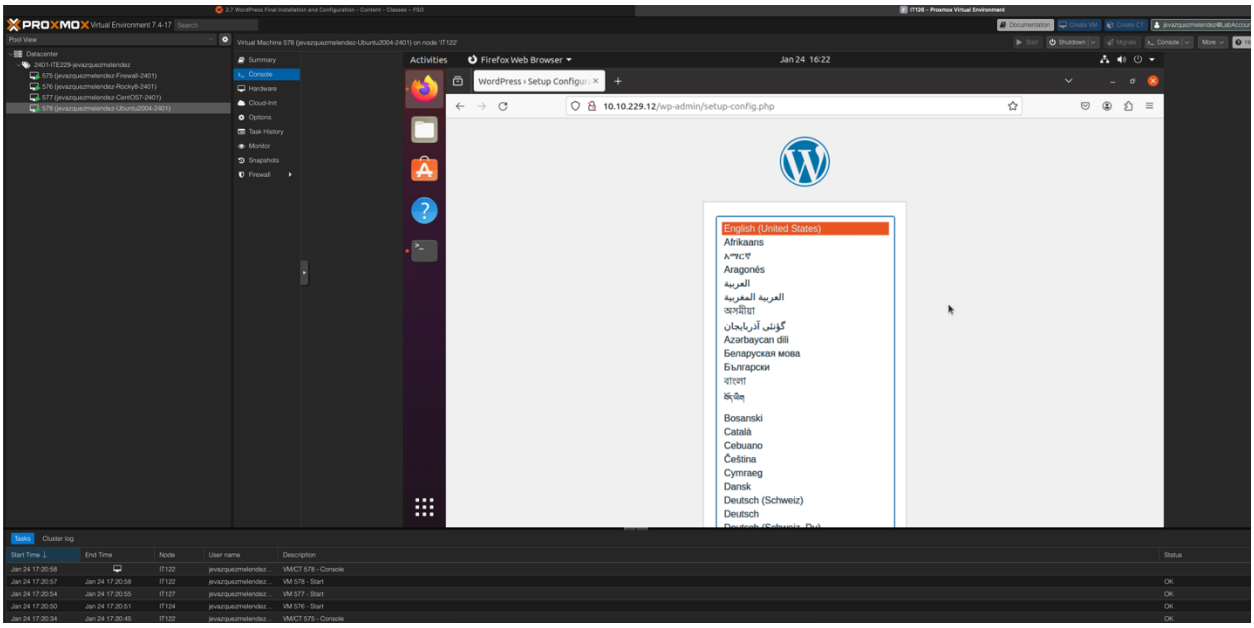
Milestone #2: WordPress Configuration

Configure WordPress

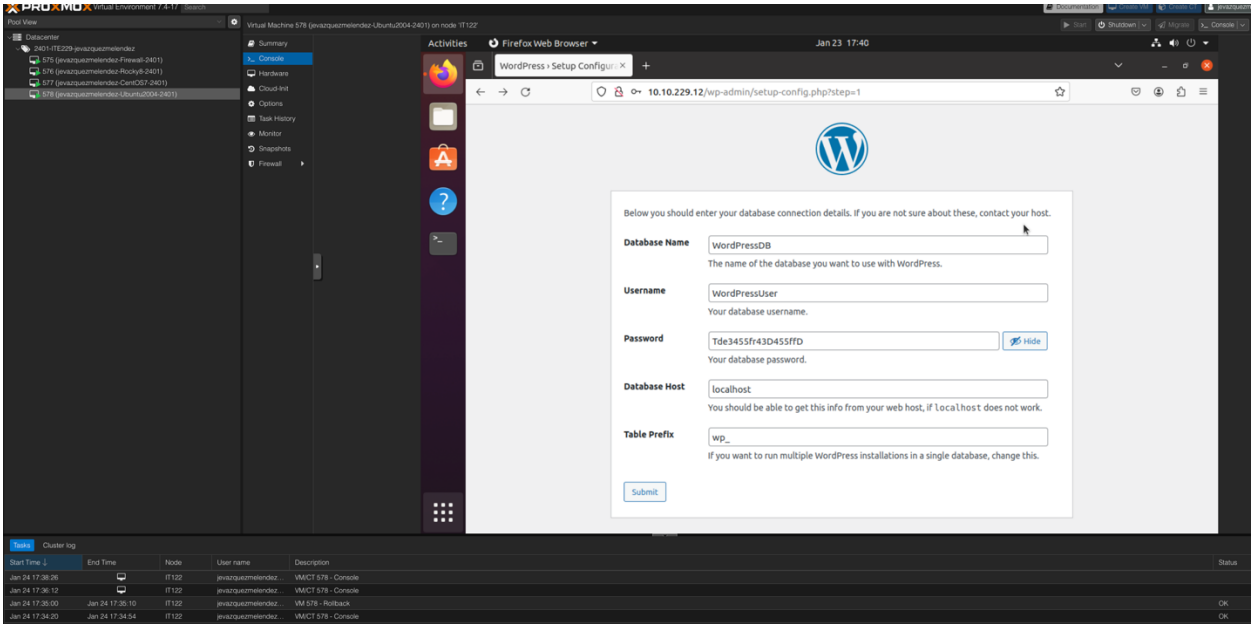
WordPress Configuration Selections

If we browser to http://10.10.229.12 it is going to take us to the Word Press Installation Process.

The first Step is to select the language.



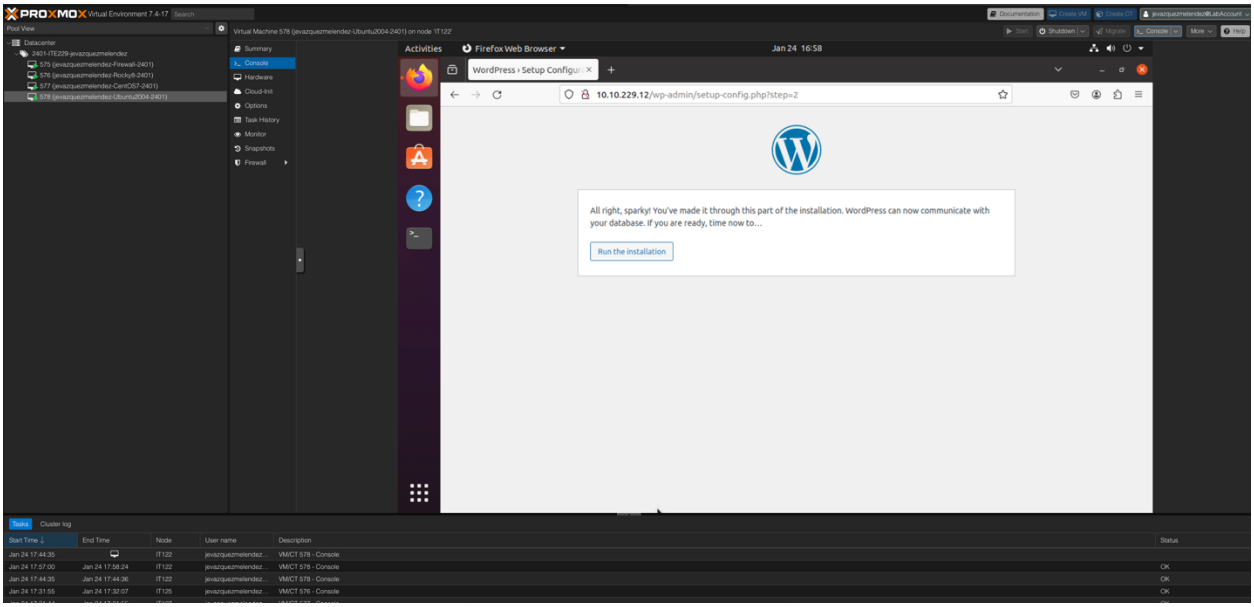
Then we must type the Data Base information we provided.
This will allow us to go ahead and proceed with the installation process.



- **Database Name:** WordPressDB
- **Username:** WordPressUser
- **Password:** Tde3455Fr43D455ffD
- **Database Host:** localhost
- **Table Prefix:** wp_

Run Installation

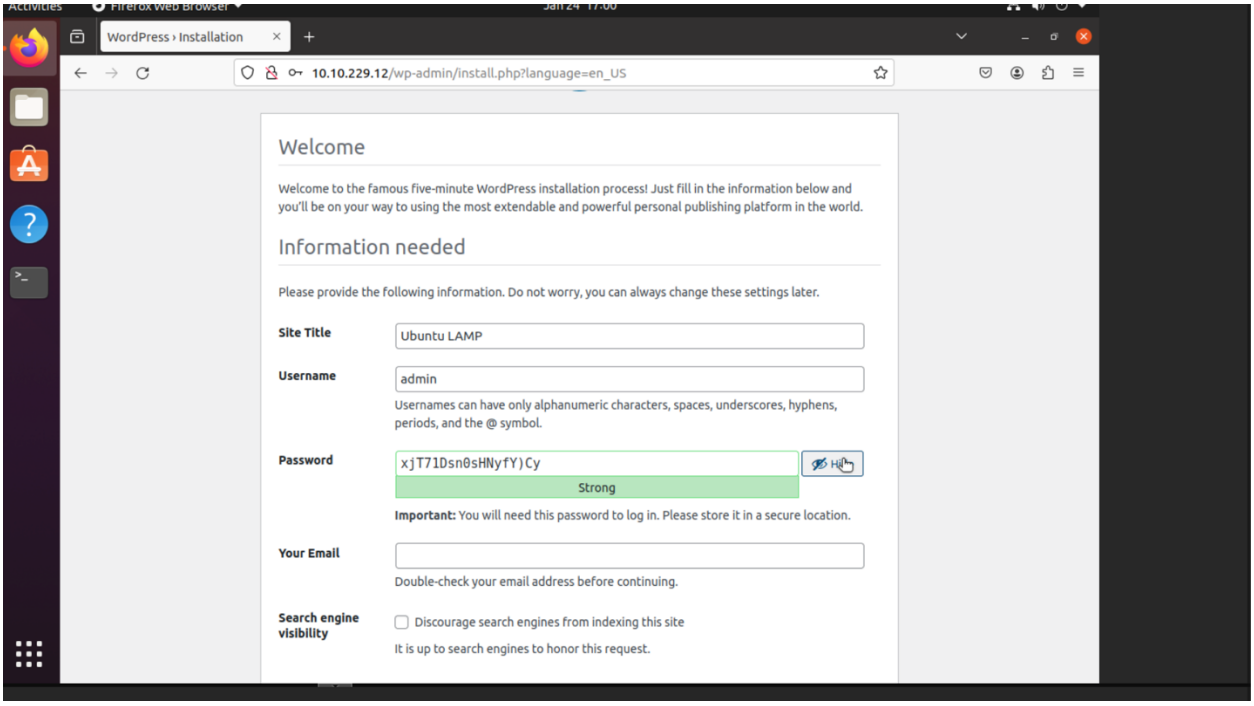
This is the prompt to RUN THE INSTALLATION of Word Press once the data base information is mapped correctly to the LAMP Stack.



Create an Admin WordPress User

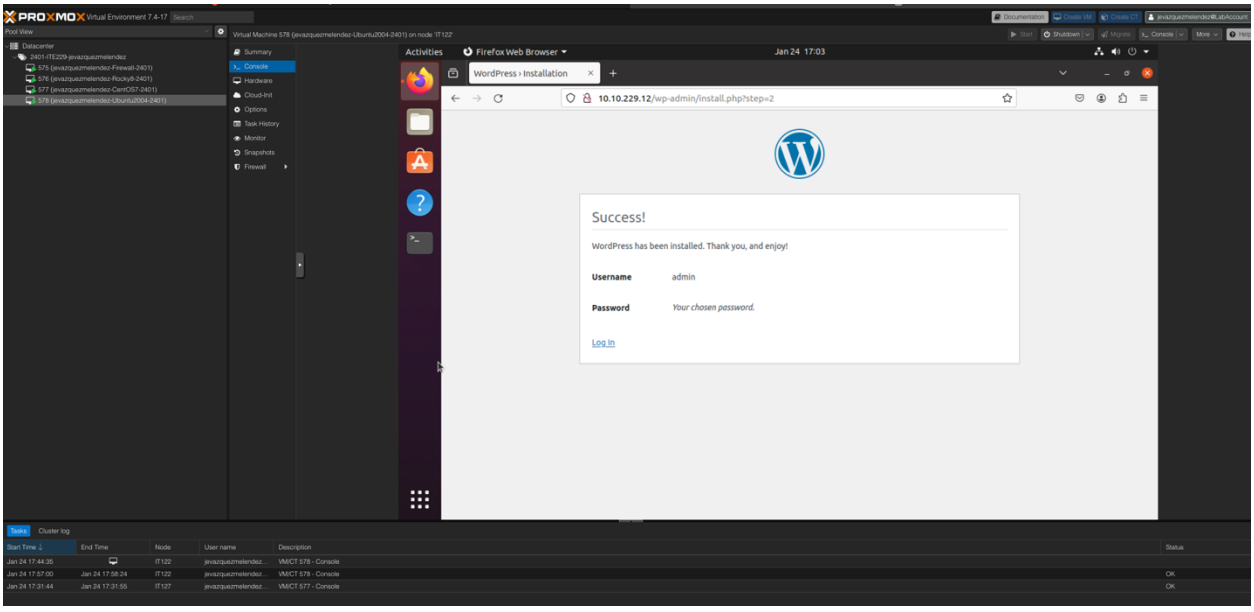
We need to create a WordPress User account.

To Create an account, Enter the information prompted.



Success!

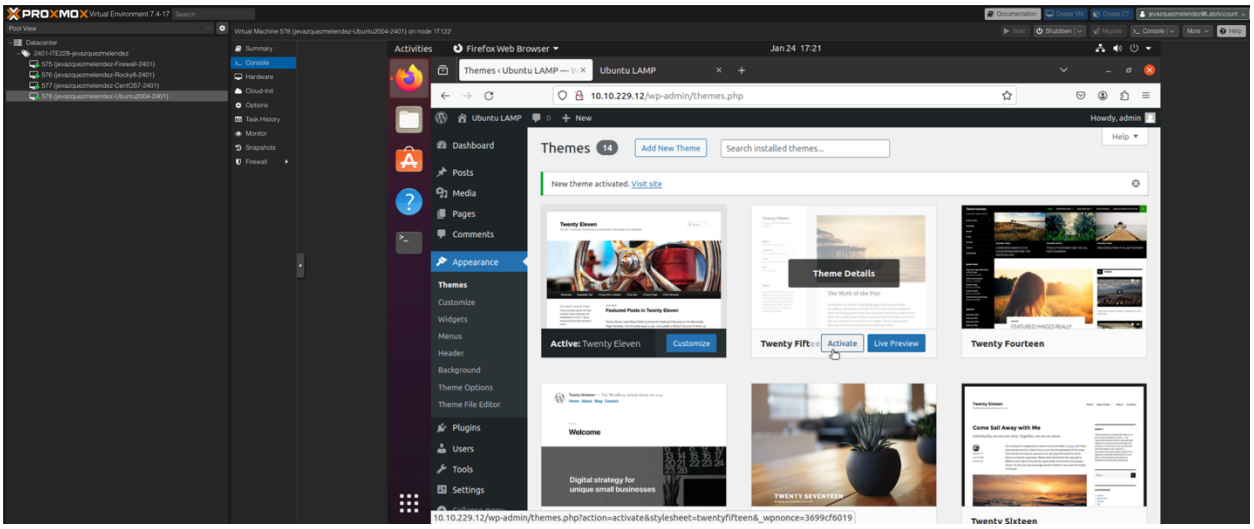
The credentials are successfully created, and you can go ahead and press Log in.



WordPress Site Selections

After successfully Logged in the WordPress Account we just created we can see the WordPress Dashboard.

To change the appearance, scroll to the Paint Brush that shows “Appearance” and a “Themes” tab should appear press it to show the default website pages you can select from.

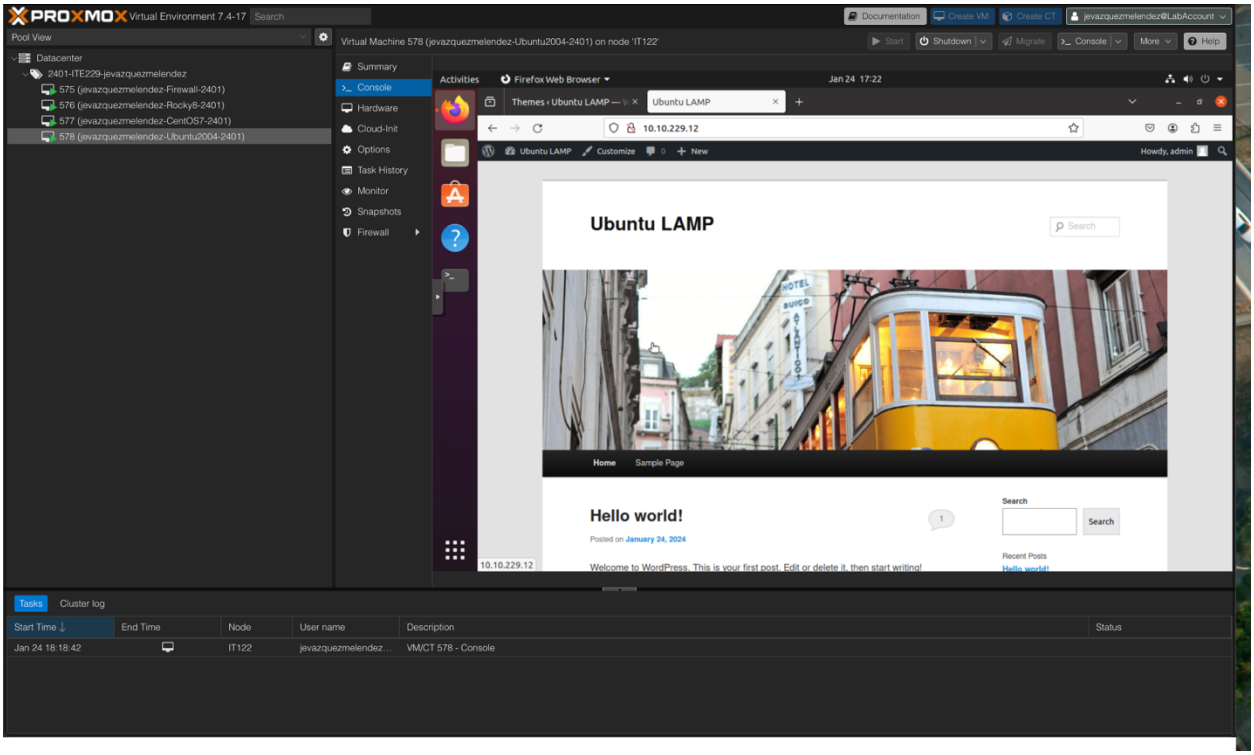


Site Title: Ubuntu LAMP
Username: admin
Password: *xjT71Dsn0sHNyfY)Cy*
Your email: root@localhost.local
Search Engine Visibility: leave unchecked

Test WordPress

To Test the Page, open a new Firefox Web Browser window, and type http://10.10.229.12

The main page with the tittle “Ubuntu LAMP” should appear as all the setting are properly configured.



IMPORTANT: To earn full credit, original formatting of this document must remain in place. In addition, ALL screenshots must include a "full view", including your ProxMox title bar with your username showing.

Milestone #3: WordPress Security & Configurations

WORDPRESS SECURITY SUMMARY

Exemplary: HALF PAGE WordPress security summary FULLY DISCUSSING what you secured on your blog site. MINIMUM: **300 words required—not including references. Include at least two (2) research references.**

DEFENSE-IN-DEPTH

Exemplary: HALF PAGE FULLY discussing how you applied defense-in-depth to this exercise. MINIMUM: MINIMUM: **300 words required—not including references. Include at least two (2) research references.**

FILE PERSMISSIONS

Before and After Screenshots AND written instructions required; Include at least two (2) sentences per screenshot.

a. Vulnerability (show screenshot and explain why this is a vulnerability)

b. Configuration (show screenshot and explain the steps you took to config changes)

c. Validation (show screenshot and explain the step you took to validate/confirm)

SECURING WP-CONFIG.PHP

Before and After Screenshots AND written instructions required; Include at least two (2) sentences per screenshot.

a. **Vulnerability** (show screenshot and explain why this is a vulnerability)

b. **Configuration** (show screenshot and explain the steps you took to config changes)

c. **Validation** (show screenshot and explain the step you took to validate/confirm)

FIREWALL (Shield)

Before and After Screenshots AND written instructions required; Include at least two (2) sentences per screenshot.

a. **Vulnerability** (show screenshot and explain why this is a vulnerability)

b. **Configuration** (show screenshot and explain the steps you took to config changes)

c. **Validation** (show screenshot and explain the step you took to validate/confirm)

CONCLUSION

Exemplary: HALF PAGE conclusion FULLY DISCUSSING how you applied security methodology and how you might apply it to other systems. MINIMUM: **300 words required—not including references. Include at least two (2) research references.**

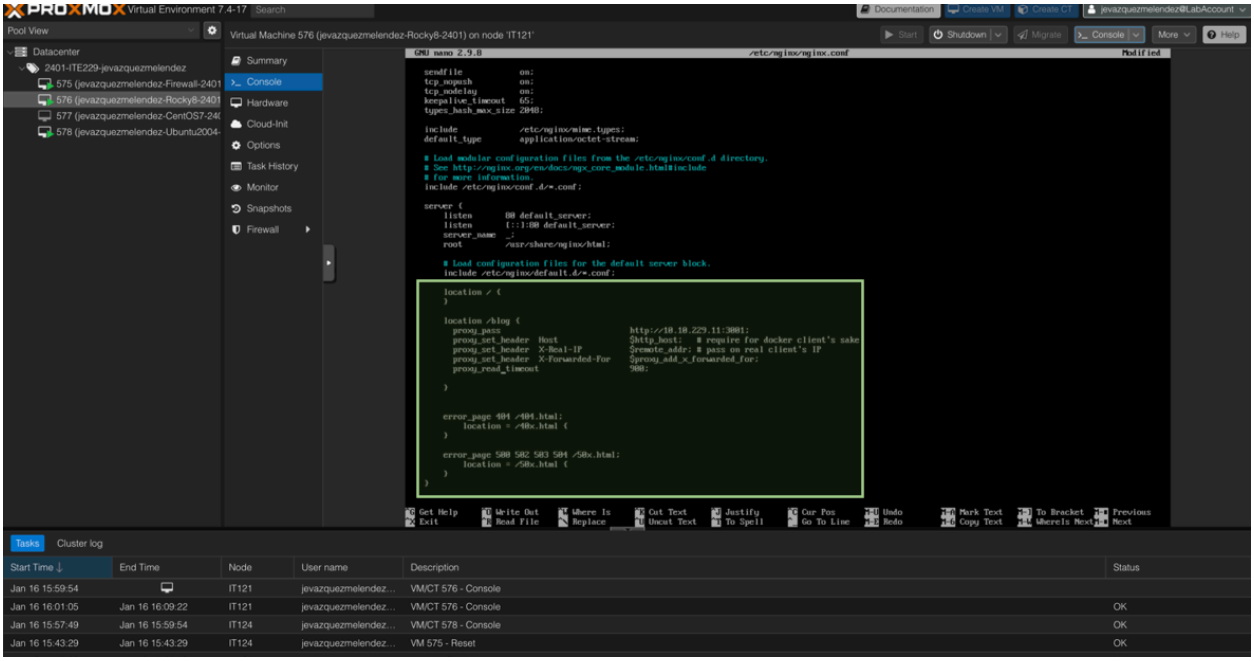
IMPORTANT: To earn full credit, original formatting of this document must remain in place. In addition, ALL screenshots must include a “full view”, including your ProxMox title bar with your username showing.

Appendix A - (Milestone #1)

NginX Config File (Include screenshot & explain)

You must follow a few simple steps to edit thx configuration file for a web server like Ghost. First, you need to locate the configuration file on your server. This file is typically located in the /etc/nginx/nginx.conf directory. Once you have located the file, you can open it using a text editor Nano.

Next, you must find the relevant section of the configuration file that you want to modify. This could include server settings, SSL configurations, or proxy settings. Once you have located the relevant section, you can make the necessary changes to the file.



Appendix B - (Milestone #1)

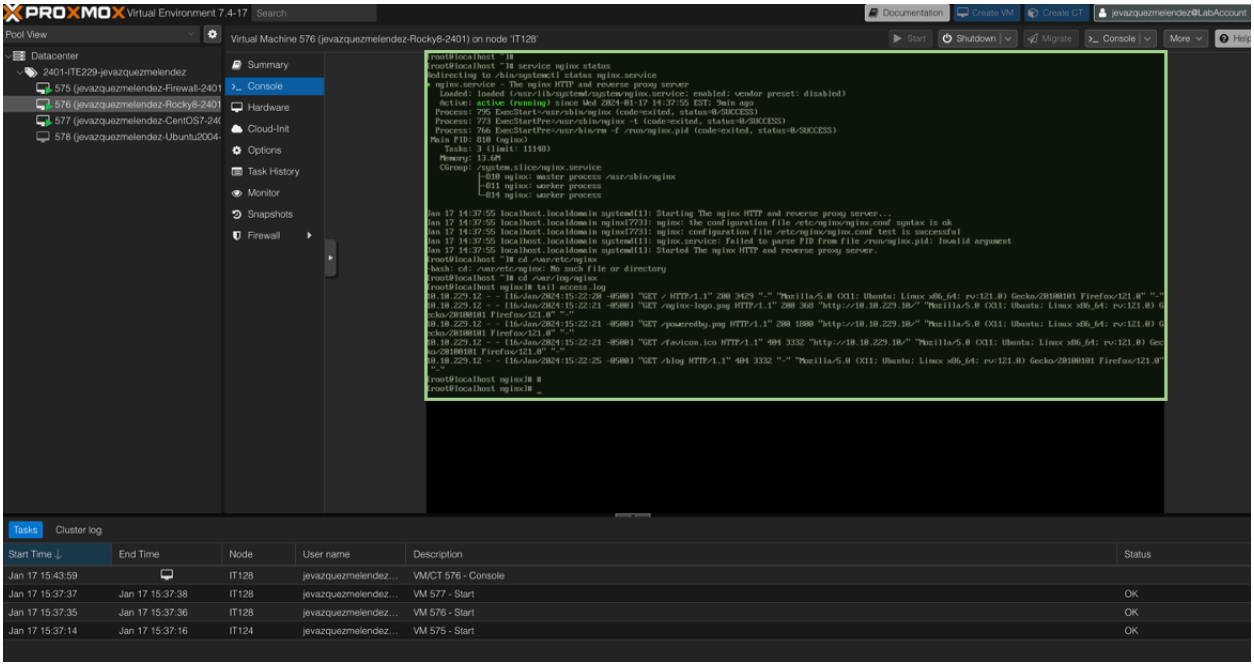
NginX Access Log File

cd /var/log/nginx

This command "cd /var/log/nginx" is used to change the current directory to "/var/log/nginx". "cd" stands for "change directory" and "/var/log/nginx" is the path of the directory we want to change to.

tail access.log

This command is used to display the last few lines of the "access.log" file. "tail" is a command that displays the last few lines of a file, and "access.log" is the name of the file we want to display. By default, "tail" displays the last 10 lines of a file.



NginX Error Log File

Page Not Found error on a website means that the web server cannot locate the requested resource or file. This error is commonly known as a 404 error, and it occurs when the web server fails to find the requested page or resource on the server.

As a website administrator, you can do a few things to troubleshoot a 404 error. First, you should check the URL to ensure it is correct and point to the correct file or resource. You should also check the server logs to see if any error messages can give you a clue as to what went wrong.

If the issue is due to a deleted or moved file, you should restore the file or update the URL to point to the correct location. If the problem is due to an incorrect server configuration, you should review the configuration files and make any necessary changes.